دراسات استراتيجية

131

راشد بشير إبراهيم

التحقيق الجنائي في جرائم تقنية المعلومات

دراسة تطبيقية على إمارة أبوظبي



مركز الإمارات للدراسات والبحوث الاستراتيجية

التحقيق الجنائي في جرائم تقنية المعلومات

التحقيق الجنائي في جرائم تقنية المعلومات

دراسة تطبيقية على إمارة أبوظبي

مركز الإمارات للدراسات والبحوث الاستراتيجية

أنشئ مركز الإمارات للدراسات والبحوث الاستراتيجية في 14 آذار/ مارس 1994، كمؤسسة مستقلة تهتم بالبحوث والدراسات العلمية للقضايا السياسية والاقتصادية والاجتماعية المتعلقة بدولة الإمارات العربية المتحدة ومنطقة الخليج والعالم العربي. وفي إطار رسالة المركز تصدر دراسات استراتيجية كإضافة جديدة متميزة في المجالات السياسية والاقتصادية والاجتماعية.

دراســات استراتيجيــة

التحقيق الجنائي في جرائم تقنية المعلومات
دراسة تطبيقية على إمارة أبوظبي

راشد بشير إبراهيم

العــدد 131

تصــدر عــن



مركـز الإمـارات للـدراسـات والبحـوث الاسـتـراتيجيـة

محتوىٰ الدراسة لا يعبِّر بالضرورة عن وجهة نظر المركز

الطبعة الأولى 2008

ISSN 1682-1203

ISBN 978-9948-00-960-3

توجه جميع المراسلات إلى رئيس التحرير على العنوان التالي:

دراسات استراتيجية - مركز الإمارات للدراسات والبحوث الاستراتيجية

ص. ب: 4567

أبوظبي - دولة الإمارات العربية المتحدة

هاتف: 4044541-9712+

فاكس: 4044542-9712+

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

المحتويات

مقدمة

لعل أهم ما يميز العصر الحالي عن غيره من العصور، هو ما نشهده اليوم من تطور مثير في المجالات التكنولوجية، الأمر الذي انعكس على مجمل مناحي الحياة، بحيث نستطيع القول بثقة بأنه لم يعد هناك شأن يتصل بالحياة الإنسانية إلا ناله نصيب من هذا التطور التكنولوجي المثير الذي أحدث ثورة أدخلت البشرية في عصر جديد. وكما هو الحال في العصور المنصرمة، فمع كل تطور في الوسائل والأدوات صاحبه تغيير في المفاهيم وأنماط السلوك البشري، وهو ما نحن بصدده الآن.

ففي نهاية القرن الماضي شهد المجتمع الإنساني تطورات تكنولوجية متسارعة شكلت الثروة الحقيقية للأمم والشعوب، وأصبحت هذه المجتمعات جزءاً لا يتجزأ من عالم المعرفة والمعلومات التي دخلت في التفاصيل اليومية لحياة الفرد والجماعة في القرن الحادي والعشرين.

وبما أن الجريمة ظاهرة اجتماعية تعكس الواقع وتتفاعل مع متغيراته وتستجيب لتطوره، فقد أفرزت هذه الابتكارات جرائم جديدة غير معتادة، عكست هذا الواقع واستخدمت أدواته واتصفت بسماته، حتى إنها اقترنت باسمه، فأطلق عليها بعضهم جرائم الحاسب الآلي والإنترنت تجاوباً مع هاتين التقنيتين اللتين تعدان عنوان هذا العصر وركيزة تطوره، أو جرائم تقنية المعلومات وهي التسمية التي اعتمدها الباحث، تناغماً مع مصطلح "عصر تقنية المعلومات".

إن من أبرز الأضرار التي تلحق بالمجتمع جراء هذا النوع من الجرائم التي أخذت تنتشر على نطاق واسع، هو ما تتكبده الشركات والمؤسسات العامة والخاصة من خسائر اقتصادية باهظة، فضلاً عن المخاطر الاجتماعية والأمنية التي تنجم عنها، الأمر الذي يفرض تحديات كبيرة على سلطات التحقيق وأجهزة العدالة الجنائية تتطلب منها اتخاذ الإجراءات والتدابير الكفيلة لمواجهتها والحد من مخاطرها، وهو ما تنصب عليه هذه الدراسة التي تعالج الجوانب المتعلقة بعملية التحقيق الجنائي في جرائم تقنية المعلومات في إمارة أبوظبي بأبعادها الإجرائية والفنية والتشريعية.

مشكلة الدراسة

فرض ظهور هذا النوع من الجرائم على جهات التحقيق تحديات عظيمة لم يسبق لها مثيل، فما تتميز به جرائم تقنية المعلومات من حيث السهولة والسرعة الفائقة في تنفيذ الجريمة، وانعدام الآثار المادية للجريمة، وغياب الدليل المرئي، وصعوبة الوصول إلى الدليل بالوسائل الفنية التقليدية، وكذلك سهولة إتلاف الدليل المادي وتدميره في زمن قياسي، كل ذلك استوجب إعادة النظر بوسائل المكافحة التقليدية للجريمة وأساليبها وطرق الوقاية منها، وأصبح من الضرورة بمكان وضع الخطط والبرامج الاستراتيجية لتحديث أجهزة العدالة الجنائية وتطويرها من حيث بنيتها المؤسسية وكوادرها البشرية لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم ومواجهة مرتكبيها وضبطهم وتقديمهم للعدالة،

فضلاً عن إشكالية مدى توافر المعرفة القانونية لدى الجهات المختصة بمواجهة هذا النوع من الجرائم، في ضوء صدور قانون جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة مؤخراً.

ومن ثم، فإن هذه الدراسة تعالج موضوع قدرات أجهزة التحقيق الجنائي وإمكاناتها بإمارة أبوظبي(القيادة العامة لشرطة أبوظبي) في التعامل مع هذا النوع من الجرائم، حيث يمكن صياغة المشكلة على شكل التساؤل الآتي: هل يمكن اعتبار المستوى التقني والمعرفي للعاملين في مجال التحقيق الجنائي كافياً للتعامل بكفاءة وفاعلية ومشروعية مع هذا النوع من الجرائم؟

أهمية الدراسة

تكمن أهمية هذه الدراسة في أنها تتصدى لظاهرة جرائم تقنية المعلومات بوصفها من الجرائم المستحدثة التي بدأت تشكل خطورة كبيرة على الاقتصادات المحلية والعالمية منذ العقد الأخير من القرن الماضي، فهذا النوع من الجرائم لم يكن معروفاً لرجال القانون والقضاء وأجهزة الشرطة والنيابة العامة، مما يتطلب إعادة النظر في وسائل المكافحة التقليدية وطرقها، وابتكار أساليب جديدة لوقاية فعالة وناجعة لمواجهة هذا النوع من الجرائم. كما أن هذه الدراسة تتناول أساليب التعامل مع الضحايا من الأطفال وطرقه باعتبارهم من الفئات المستهدفة، خاصة أن دولة الإمارات العربية المتحدة، التي تعد إمارة أبوظبي إحدى الإمارات السبع التي يتكون منها الاتحاد وأكبرها مساحة وسكاناً، هي في مقدمة الدول العربية من حيث استخدام

الوسائل التقنية الحديثة، وتسير بخطى حثيثة لتكريس مفهوم الحكومة الإلكترونية تحت شعار "مؤسسات بلا أوراق".

أهداف الدراسة

ترمي هذه الدراسة إلى تحقيق الأهداف الآتية:

1. تحديد جوانب القوة والضعف في معالجة أوجه الخلل الذي تعانيه أجهزة العدالة الجنائية في إمارة أبوظبي لمواجهة هذا النوع من الجرائم.
2. اقتراح الآليات المناسبة لرفع كفاءة الأجهزة المختصة وفاعليتها في مواجهة هذه الجرائم بإمارة أبوظبي.
3. التنبيه لأهمية تطوير التشريعات الجزائية بما يتلاءم مع التطور المطرد لجرائم تقنية المعلومات.
4. التنبه لضرورة التعاون الدولي كآلية فعالة للتصدي لهذه الظاهرة.

تساؤلات الدراسة

تجيب هذه الدراسة عن التساؤلات الآتية:

1. إلى أي مدى تستطيع أجهزة العدالة الجنائية بإمارة أبوظبي التعامل من الناحية الفنية مع جرائم تقنية المعلومات؟
2. هل المحققون الجنائيون بمراكز الشرطة في إمارة أبوظبي مؤهلون للتعامل مع هذا النوع من الجرائم؟

3. هل التشريعات الجزائية الحالية بشقيها الإجرائي والموضوعي بدولة الإمارات العربية المتحدة كافية لتغطية الجوانب القانونية المتصلة بهذه الظاهرة؟

4. هل المحققون الجنائيون بالقيادة العامة للشرطة بإمارة أبوظبي على إلمام بالتشريعات الجزائية بشقيها الإجرائي والموضوعي المتعلقة بهذا النوع من الجرائم؟

5. ما الوسائل التي ينبغي اتباعها للتعامل مع الجريمة المعلوماتية الموجهة ضد الأطفال بإمارة أبوظبي؟

فرضيات الدراسة

تقوم هذه الدراسة على اختبار الفرضيتين الآتيتين:

الفرضية الأولى:

أ. فرضية العدم: إن أجهزة العدالة الجنائية في إمارة أبوظبي مؤهلة تأهيلاً كافياً للتعامل مع جرائم تقنية المعلومات (Ho).

ب. الفرضية البديلة: هذه الأجهزة ليست مؤهلة وغير قادرة من الناحية الفنية للتعامل مع هذا النوع من الجرائم (Hi).

الفرضية الثانية:

أ. فرضية العدم: التشريعات الجزائية بدولة الإمارات العربية المتحدة تغطي كافة الجوانب القانونية، وهي كافية بشقيها الإجرائي والموضوعي لمواجهة جرائم تقنية المعلومات (Ho).

ب. الفرضية البديلة: هذه التشريعات يعتريها النقص وهي غير كافية لمواجهة هذا النوع من الجرائم (Hi).

منهجية الدراسة

يتوقف المنهج العلمي الذي يتبعه الباحث في دراسته على طبيعة الظاهرة التي يتناولها والإشكالية التي يعالجها، ونظراً لطبيعة هذه الدراسة القائمة على معطيات نظرية تتعلق بظاهرة جريمة تقنية المعلومات، فقد لجأ الباحث إلى المنهج التحليلي الوصفي في تحليل مفاهيم هذه الظاهرة وإجراءات التحقيق فيها وحصر مشكلاتها وتحليلها واختبار الفرضيات وتحديد العلاقة بين متغيراتها، كما استعان الباحث بالمنهج التحليلي الكمي في دراسته المسحية لعينة من المحققين لإثبات فرضيات الدراسة المتعلقة بقدراتهم التقنية في مواجهة هذه الظاهرة.

تعريف مصطلحات الدراسة والدراسات السابقة

أولاً: تعريف مصطلحات الدراسة

الحاسب الآلي Computer:

المعنى اللغوي: حَسَبَ الشَّيْءَ أي قَدَّرَه، وحسب حسبةً وحساباً وحسباناً: عدَّه، والمعدود محسوب، والحاسب الآلي: استخدام آلة أو جهاز مخصص للحساب والعد.[1]

المعنى الاصطلاحي: جهاز يقوم بعمليات حسابية آلية، ويعمل على معالجة المعلومات التي يتم إدخالها فيه، ويقوم بإعطاء النتائج المطلوبة منه، ومعالجة البيانات وتفسيرها بحسب البرامج المدخلة إليه، وقد عرف القانون الأمريكي الحاسب الآلي «بأنه جهاز إلكتروني بصري كيميائي كهربائي لإعداد معلومات ذات سرعة عالية يؤدي وظائف منطقية حسابية وتخزينية، ويشتمل على تسهيل لتخزين المعلومات أو تسهيل اتصالات مباشرة مقترنة أو تعمل بالاقتران مع هذا الجهاز».[2]

في ضوء ذلك، فإن عمل جهاز الحاسب الآلي يتكون من ثلاث مراحل متتابعة هي:

مدخلات ← معالجة ← مخرجات

1. المدخلات Input: هي البيانات التي يتم إدخالها في الجهاز.

2. المعالجة Process: وهي العمليات التي يقوم بها الجهاز لإيجاد الحلول المنطقية للبيانات المدخلة وفق البرنامج المخزن بالجهاز.

3. المخرجات Output: وهي النتيجة والمحصلة النهائية التي يطرحها الجهاز للعمليات التي يقوم بها.

أما نظام الحاسب الآلي فيتكون من:

1. المكونات المادية Hardware، وتشتمل على الشاشة ولوحة المفاتيح ووحدة المعالجة المركزية (CPU).

2. البرامج والتطبيقات Software، وتشتمل على البرامج والتطبيقات اللازمة للتشغيل ومعالجة البيانات المدخلة.

3. البيانات (DATA)، وهي المادة الخام للمعلومات المطلوب معالجتها.

تقع الجريمة المعلوماتية عندما يتم الاعتداء على نظام عمل الجهاز كالدخول غير المشروع أو التلاعب بالمدخلات أو العمليات أو النتائج، وكذلك تقع الجريمة بالاعتداء على مكونات الجهاز نفسه.[3]

الإنترنت Internet الشبكة العالمية:

تتكون كلمة "الإنترنت" من مقطعين؛ الأول إنتر Inter، وهي اختصار لكلمة دولي International، والثاني نت Net، وهي اختصار لكلمة Network، وتعني الشبكة.[4] وتقوم الشبكة الدولية "الإنترنت" على مجموعة هائلة من أجهزة الحاسب الآلي المتصلة معاً، تشكل شبكات من الاتصال الفردي والجماعي، وهي مرتبطة فيما بينها بما يشبه خيوط العنكبوت. هذه الأجهزة الموزعة والمتناثرة في أنحاء العالم جميعها تحمل سمات الاتحاد الكونفيدرالي؛ فهي مستقلة ومترابطة في آن معاً، وهي ليست مملوكة لأفراد أو مؤسسات بعينها.[5]

يرجع تاريخ نشأة الشبكة الدولية "الإنترنت" إلى الستينيات من القرن الماضي، حيث أنشأتها الولايات المتحدة الأمريكية لخدمة الأغراض العسكرية، كثمرة لجهود وكالة تنمية البحوث العسكرية التابعة للجيش

الأمريكـي Advanced Research Projects Agency، وكـان اسـتخدامها مقتصراً على مجال التأهب السريع للقوات المسلحة في حـال نـشوب حـرب نووية أو أي هجوم عسكري قد تتعرض له الولايات المتحدة الأمريكيـة، إلا أنه وبعد زوال خطر التهديد النووي في إثر انهيار الاتحاد الـسوفيتي في مطلـع التسعينيات من القرن الماضي، قلت أهمية الغـرض العـسكري لهـذه الـشبكة وأصبح المجال مفتوحاً أمام الاسـتخدامات المدنية.

وجدير بالذكر أن نائـب الـرئيس الأمريكـي الأسـبق آل جـور Albert Algore كان أول من فكر في استخدام إمكانات شبكة الإنترنت عـلى نطـاق عالمي مدني، وأنشأ ما يعرف بطريق المعلومات الفائق الـسرعة Information Superhighway.[6]

العلاقة بين الإنترنت والحاسب الآلي

من الواضح أن التطور الهائل الذي طرأ على أجهـزة الحاسـب الآلي قـد أحـدث ثـورة في مجـال الاتـصالات وتخـزين المعلومـات ومعالجتهـا، ومـن المعروف أن اختراع الحاسب الآلي كان سابقاً لوجود شبكة الإنترنت، لـذلك فإن هذه الشبكة قد أطلت علينا من نافذة الحواسيب الآليـة، وهـو مـا يظهـر وجه الارتباط فيما بينهما.[7] وفي الحقيقة ليس بمقدورنا الاستفادة من الخدمات الهائلة والعظيمة لشبكة الإنترنت إلا من خـلال جهـاز الحاسـب الآلي الـذي تزداد أهميته والحاجة إليه مع اتساع استخدام شـبكة الإنترنـت عـلى النطـاق العالمي.

القراصنة Crackers

يقصد بالقراصنة الأشخاص الذين يقدمون على استخدام أو نسخ غير مشروع لنظم التشغيل أو البرامج المختلفة للحاسب الآلي المحمية بموجب قوانين حق المؤلف، سواء بالاستفادة منها شخصياً أو تجارياً، تحقيقاً لأهداف أو ميول إجرامية، وطبقاً لإحصائية اتحاد منتجي البرامج في الولايات المتحدة الأمريكية لعام 2000، فإن نسبة القرصنة وصلت إلى 56٪ وقدرت الخسائر الناجمة عن ذلك بحوالي 12 مليون دولار، الأمر الذي يؤكد خطورة هذا النوع من المجرمين على الاقتصادات المحلية والعالمية.[8]

المتسللون Hackers

هم أشخاص برعوا في استخدام الحاسب الآلي وبرامجه ولديهم فضول وحب استكشاف يدفعهم للدخول إلى أجهزة الحاسب الآلي للآخرين بطرق غير مشروعة، وبدافع التطفل أو التحدي وإثبات المقدرة على اختراق نظم أمن الشبكات. وفي الغالب، فإن أفعالهم هذه لا تحمل ميولاً إجرامية أو نوايا تخريبية.[9]

ويلاحظ أن مخاطر المتسللين في الآونة الأخيرة قد تعدت حدود التطفل والتحدي، بأن ازدادت بصورة تثير الهلع لدى الهيئات الحكومية والخاصة، حيث صدر تحذير لخبير في شؤون أمن الحاسب الآلي التابع لمنظمة استخبارية ينبه لمخاطر أنشطة المتسللين التي قد تصيب كل شيء بالجمود، الأمر الذي أدى بالسلطات الأمنية الأمريكية إلى الدعوة إلى اجتماع على مستوى حكام

الولايات مع قيادات وزارة العدل الأمريكية لمواجهة المخاطر المتوقعة على شبكة الإنترنت ممن سموا أنفسهم اللوديين Luddites، وهم متسللون مهرة كرسوا أنفسهم لتعطيل الأجهزة والوسائط الإلكترونية.[10]

الفيروسات Viruses

فيروس الحاسب الآلي هو عبارة عن برنامج كتب بإحدى لغات البرمجة، أعده مبرمجون متخصصون، وهو قادر على التوالد والتناسخ ويستطيع الدخول إلى البرامج، ويتفوق على نظم التشغيل، ويصل إلى المكونات المادية مثل الذاكرة الرئيسية أو القرص الصلب، ويهدف الفيروس إلى الولوج للبرامج وتخريبها والانتشار فيها بقوة، كما أن له خاصية الاختفاء والظهور، ولديه القدرة على التزايد والانتشار، ويضرب بمجرد كتابة كلمة أو إصدار أمر، أو حتى بمجرد فتح البرنامج الحامل للفيروس أو الرسالة البريدية، مما يؤدي إلى إصابة الجهاز ومسح محتوياته أو العبث بالملفات المخزنة.[11]

ويتميز الأشخاص الذين يرتكبون هذه الأعمال بمقدرة عالية على تصميم البرامج الحاملة للفيروس وإطلاقها، وتعد هذه الاعتداءات من أشد المخاطر التي تصيب أجهزة الحاسب الآلي نظراً لما ينتج عنها من أضرار وخسائر بالغة الكلفة، وهي قادرة على إصابة جميع الأعمال المرتبطة بالحاسب الآلي بالشلل التام.

القنابل المنطقية أو الموقوتة Time Bombs, logic Bombs

وهي عبارة عن برنامج يصمم للدخول إلى النظام المعلوماتي وينتشر بداخله، بحيث تبقى ساكنة وغير فعالة مدة قد تصل إلى أشهر أو أعوام وقد تنشط بتاريخ معين كأول يناير أو إبريل أو نتيجة ظرف منطقي كتغيير أمر ما أو محو اسم أو إدخال أو معالجة معلومة، بحيث تعمل على تدمير النظام كلياً أو جزئياً.[12]

ثانياً: الدراسات السابقة

على الرغم من قلة الكتب والإصدارات التي تناولت جرائم الحاسب الآلي والإنترنت في عالمنا العربي نظراً للحداثة النسبية لهذا النوع من الجرائم، فإن عدداً من الباحثين تناول هذه الظاهرة من جوانب متعددة؛ فبعضهم تناولها من منظور أمني، وآخرون من منظور إسلامي، وغيرهم من منظور تشريعي، وسوف نستعرض فيما يلي أهم هذه البحوث التي تناولت هذه الظاهرة.

تناول يونس عرب هذه الظاهرة في بحثه "جرائم الكمبيوتر والإنترنت: إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات" المقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي انعقد بجامعة الإمارات العربية المتحدة من 1- 3 أيار/ مايو 2000 مستعرضاً المفاهيم المتعلقة بهذه الجرائم، وأشار إلى بعض

المشكلات التي تواجه الملاحقة القضائية للمجرمين، وأوصى باتباع بعض الإجراءات المتعلقة بالضبط والتفتيش.

كما تناول هشام محمد زيد رستم هذه الجرائم في بحثه "الجرائم المعلوماتية أصول التحقيق الجنائي الفني" المقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي انعقد بجامعة الإمارات من 1- 3 أيار/ مايو2000 ، حيث نبه لأهمية الاتفاق على آلية عربية موحدة للتدريب التخصصي لمواجهة هذه الظاهرة، واستعرض تعريفات للجريمة المعلوماتية عديدة.

وعالج إسماعيل عبد النبي في بحثه "أمن المعلومات في الإنترنت بين الشريعة والقانون" المقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي انعقد بجامعة الإمارات من 1- 3 أيار/ مايو 2000 موضوع تعريف الإنترنت وتاريخ ظهورها وعلاقتها بالحاسب الآلي، وتطرق للأمن التقني للمعلومات (الحماية السرية) من خلال مفهوم الجدار الناري الذي يمنع دخول المستخدمين غير المصرح لهم إلى الشبكة وهو نظام حماية عامة ضد الهجمات جميعها التي يمكن أن تتعرض لها الشبكة، وتطرق أيضاً إلى التشفير كتقنية مستخدمة في أمن المعلومات في الإنترنت، وتعرض الباحث لأهم صور الاعتداء على المعلومات؛ كجريمة النصب والاحتيال، والتجسس، والعبث بالأنظمة، وسرقة حقوق الملكية الفكرية وقارن بينها وبين الاعتداء على حق مالي ومعنوي في الفقه الإسلامي، وأشار الباحث إلى أوجه الشبه بين خصائص الحق المالي المعتدى عليه في هذا النوع من الجرائم وبين جريمة الغصب التي تستوجب التعزير في الفقه الإسلامي.

أما محمد عبدالرحيم سلطان وفي بحثه "جرائم الإنترنت والاحتساب عليها" المقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي انعقد بجامعة الإمارات من 1- 3 أيار/ مايو 2000 فقد تناول الظاهرة من منظور إسلامي مبيناً خصوصيتها من حيث صعوبة الإثبات، واستعرض أنواع هذه الجرائم والجهات المخولة للاحتساب عليها وقسمها بحسب تصنيفه إلى ثماني مجموعات نعرض منها:

- اختراق شبكات الحاسب الآلي وأجهزته، والجهة المخولة للاحتساب عليها هي وزارة المواصلات.
- التجسس، الجهة المخولة للاحتساب عليها وزارتا الدفاع والداخلية.
- التخريب والإتلاف، الجهة المخولة للاحتساب عليها وزارتا المواصلات مع الجهات الأمنية.
- التحريف والتزوير، الجهة المخولة للاحتساب عليها وزارتا المالية والاقتصاد والمواصلات.

أما بالنسبة لإمارة أبوظبي فلم يسبق أن صدرت دراسة تناولت التحقيق الجنائي والتحديات التي تواجه سلطات التحقيق وأجهزة العدالة الجنائية في مجال جرائم تقنية المعلومات. لذلك، فإن دراستنا هذه ستتناول الموضوعات ذات الصلة بالتحقيق الجنائي، والتي ستبدأ بمفاهيم جرائم تقنية المعلومات.

مفهوم جرائم تقنية المعلومات

منذ بروز جرائم تقنية المعلومات كظاهرة في العقدين الأخيرين من القرن الماضي اختلف الباحثون حول تبني مفهوم محدد لهذا النوع من الجرائم، فاعتمد بعضهم مفهوماً موسعاً، والآخرون اعتمدوا مفهوماً ضيقاً، كلٌّ بحسب نظرته للجريمة وطبيعتها ومحلها من حيث مساسها بالأشخاص أو الأموال أو المعتقدات الدينية أو الأخلاق أو الأمن القومي،[13] انطلاقاً من المفاهيم التي يؤمنون بها والقيم السائدة في المجتمعات التي ينتمون إليها، حيث نجد أن الدول الغربية التي تنتمي مجتمعاتها إلى المفاهيم الليبرالية والعلمانية، تخرج من نطاق التجريم قسماً كبيراً من الأفعال التي تشكل اعتداءً على الأخلاق والمعتقدات الدينية، تحت شعار حرية التعبير عن الرأي والحرية الشخصية.[14]

وهو ما نلحظه من خلال ما ينشر عبر شبكة الإنترنت من مواقف وأفكار تشكل اعتداء على المعتقدات والمقدسات الدينية، وما يبث من صور وأفلام فاضحة تنتهك القيم الأخلاقية والآداب العامة. وخير دليل على ذلك ما نشر مؤخراً من صور مسيئة لرسولنا محمد عليه الصلاة والسلام بصحيفة دنماركية وبث عبر شبكة الإنترنت، وما تبعه من جدل وخلاف حول معاقبة الجهة التي صدر عنها هذا الفعل، ورفض المحكمة الدنماركية قبول الدعوى التي تقدم بها ممثلو الجالية الإسلامية هناك؛ متذرعة بتعارضها مع مبادئ حرية التعبير عن الرأي التي كفلها النظام الديمقراطي لديهم.[15]

وفي المقابل، فإن الاتجاه السائد في منطقتنا العربية والإسلامية ينحو باتجاه التوسع في مفهوم جرائم تقنية المعلومات ويتبنى تصنيفات موسعة تشمل أشكال الأفعال والسلوك المخلة بالآداب العامة والقيم الأخلاقية كافة، ويمنع الإساءة للمعتقدات الدينية، ويتصدى للأفكار الداعية للرذيلة والانحلال.

وبصرف النظر عن المنطلقات التي استند إليها الباحثون في تصنيفهم لجرائم تقنية المعلومات، فإن أي تصنيف لا يقوم على أسس تشريعية ولا يستند إلى نصوص عقابية يصبح فاقد القيمة من الناحية القانونية ويبقى في إطار السجال الفقهي والأكاديمي، من هذا المنطلق سوف نقوم بتصنيف جرائم تقنية المعلومات استناداً إلى نصوص قانون تقنية المعلومات الاتحادي رقم 2 لسنة 2006 بدولة الإمارات العربية المتحدة الذي صدر مؤخراً، ولكن قبل ذلك سوف نعرض نموذجين من التصنيف: الأول يمثل المفاهيم الغربية من خلال عرض موجز للتصنيف الذي أقرته الاتفاقية الأوروبية لجرائم الكمبيوتر والإنترنت عام 2001، وتصنيف وزارة العدل الأمريكية لعام 2000. والتصنيف الثاني يمثل المفاهيم العربية والإسلامية من خلال تصنيف الباحثين يونس عرب ومحمد عبدالرحيم العلماء.

أولاً: تعريف جرائم تقنية المعلومات

لم يستقر الفقه القانوني على مفهوم محدد لجرائم تقنية المعلومات بوصفها من الجرائم المستحدثة.[16] التي ماتزال في مهد البحث والدراسة؛ فمعظم

الباحثين الذين تطرقوا لهذا النوع من الجرائم قد اعتمدوا مفاهيم تخدم أغراض بحوثهم واستخدموا أساليب ومناهج تلائم المجال الذي تنتمي إليه دراساتهم،[17] لذلك تعددت التعريفات وتفاوتت ضيقاً واتساعاً تبعاً للمعايير والمنطلقات المستندة إليها، فمنها ما اعتمد أصحابها في تعريف جرائم تقنية المعلومات على معيار الوسيلة المستخدمة في ارتكاب الجريمة، وآخرون اعتمدوا معيار موضوع الجريمة ذاتها، وغيرهم اعتمدوا معايير مختلطة ومختلفة، وسوف نستعرض فيما يلي أهم هذه التعريفات، ثم نوضح موقفنا منها والتعريف الذي نقترحه:

1. التعريف المستند إلى معيار الوسيلة المستخدمة:

تدور معظم التعريفات المنطلقة من هذا الرأي حول الحاسب الآلي بوصفه الوسيلة المستخدمة في ارتكاب هذا النوع من الجرائم، حيث يرى الفقيه الألماني كلاوس تيدمان Klaus Tiedemann أن جرائم تقنية المعلومات هي «كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي»، كما يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها «الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً».[18]

وفي السياق نفسه يعرفها الباحث ليسلي بيل Leslie D. Ball[19] بأنها: «الفعل غير المشروع الذي يكون الحاسب الآلي أداة رئيسية في ارتكابه أو مختلف السلوك الإجرامي الذي يرتكب باستخدام المعالجة الآلية للبيانات،

أو أي عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب الآلي وشبكات الاتصال الخاصة التي يجرمها قانون العقوبات».[20]

الحقيقة أن هذه التعريفات تركز جميعها على الوسيلة المستخدمة في ارتكاب الجريمة كمعيار وحيد لتعريف هذا النوع من الجرائم، ونرى أن هذا المنحى يتصف بالقصور وعدم الدقة؛ لأن العمليات الإلكترونية لا تنحصر في استخدام جهاز الحاسب الآلي، وإن كان يمثل عمودها الفقري والنافذة التي يطل بواسطتها، إلا أنه بفضل الثورة التقنية العارمة والتطوير الهائل في مجال الاتصالات، ظهرت في الآونة الأخيرة اختراعات وابتكارات تقنية متعددة، وبخاصة في مجال التجارة الإلكترونية، ودخول العمليات المصرفية إلى نطاق الاستخدامات الإلكترونية بشكل واسع؛ كالكمبيالة الإلكترونية، والشيك الإلكتروني، والنقود الإلكترونية، وبطاقات الائتمان والسحب الآلي،[21] وكذلك التعامل عبر البريد الإلكتروني، واتساع مجالات الحكومة الإلكترونية، وازدياد استخدام شبكات الإنترنت على المستويين الوطني والدولي، كل ذلك أفرز معطيات تجاوزت جهاز الحاسب الآلي كمكون مادي وإن كانت جميعها تعتمد بشكل أساس على جهاز الحاسب الآلي وشبكة الإنترنت بحيث لا يمكنها القيام بوظائفها بدونها، إلا أنها تظل أدوات منفصلة، يمكن أن تكون بحد ذاتها محل جريمة، أو تستخدم لارتكاب جريمة، لهذه الأسباب نرى أن اقتصار التعريف على معيار الأداة المستخدمة يعد تعريفاً قاصراً وغير دقيق.

2. التعريف المستند إلى معيار موضوع الجريمة:

يرى بعض الفقهاء أن الجريمة المعلوماتية ليست هي التي يكون الحاسب الآلي أداة ارتكابها بل التي تقع على جهاز الحاسب الآلي أو على برامجه، وانطلاقاً من هذا الفهم عرفها الباحث روزنبلات Rosenblatt وآخرون بأنها «النشاط غير المشروع الموجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه».[22]

وفي رأينا، فإن هذا التعريف وقع في الخطأ نفسه الذي أصاب الفريق السابق بأن ربط موضوع الجريمة بجهاز الحاسب الآلي، سواء كانت المعلومات مخزنة بداخله أو محولة عن طريقه ما دامت عملاً غير مشروع دون أن يشمل الأفعال غير المشروعة التي قد تقع على الوسائل التقنية الأخرى التي أفرزتها التطورات التقنية للمعلومات التي ذكرناها في تعقيبنا على التعريف الأول.

3. التعريف المستند إلى معايير مختلفة ومختلطة:

توجد نماذج من التعريفات تقوم على معايير مختلفة؛ منها تعريف ديفيد تومبسون David Thompson[23] الذي يعتبر أن الجريمة المعلوماتية هي «كل جريمة تتوافر في مرتكبها معرفة تقنية بالحاسب الآلي»، وقد ورد مثل هذا التعريف بصيغة أخرى في تقرير لوزارة العدل الأمريكية أعده معهد ستانفورد الدولي للأبحاث (SRI) جاء فيه «أن جريمة تقنية المعلومات هي الجريمة التي يكون لفاعلها معرفة تقنية بالحاسبات الآلية تمكنه من ارتكابها»،

أما آرثر سولارز Artur Solarz فقد اعتبر أن الجريمة المعلوماتية «نمط من أنماط السلوك غير المشروع المعروفة بقانون العقوبات طالما كان مرتبطاً بتقنية المعلومات».[24]

والحقيقة أن هذه التعريفات التي تعتمد على معايير متعددة إنما تتسم تارة بالضيق لاعتماد بعضها على العامل الشخصي كتعريف ديفيد تومبسون، وتارة بالاتساع كتعريف سولارز الذي شمل كل أنواع السلوك غير المشروع مادام مرتبطاً بتقنية المعلومات دون أهمية للقصد الجنائي. وفي كلتا الحالتين، فان التعريف لا يعبر عن المفهوم الدقيق والفعلي لجرائم تقنية المعلومات.

التعريف الذي يقترحه الباحث:

يعتقد الباحث – في ضوء ما تقدم – أن التعريف الذي يغطي الصور المختلفة لجرائم تقنية المعلومات ويعكس مدلولاتها الواقعية والتشريعية ينبغي أن يشمل العناصر الآتية:

1. الأفعال جميعها التي تلحق ضرراً باقتصاد الدولة وأمنها الداخلي والخارجي وتعتدي على القيم الأخلاقية والمعتقدات الدينية، إذا استخدمت في ارتكابها الوسائل الإلكترونية لنظم تقنية المعلومات، أو أنها وقعت على أحد مكونات هذه التقنيات.

2. تجريم هذه الأفعال وفق نصوص قانون العقوبات أو القوانين الخاصة، بما ينزع عنها صفة المشروعية.

3. توافر ركن القصد الجنائي؛ فكثير من الأفعال الضارة قد تصدر عن الهواة والأطفال بقصد اللهو أو العبث وتحدث ضرراً غير مقصود، فلا يصح أن يعامل هؤلاء كالمجرمين العتاة الذين يدركون كنه أفعالهم ويسعون لتحقيق مقاصد إجرامية.

4. الجمع بين موضوع الجريمة وأداة استخدامها، على ألا تنحصر هذه الأدوات في جهاز الحاسب الآلي فحسب، بل تشمل أيضاً وسائل تقنية المعلومات كافة ونظمها الحالية والمستقبلية.

من هذا المنطلق نرى أن التعريف الذي نعتقد أنه يخدم هذه الأغراض ويعبر بصورة وافية ودقيقة عن المدلولات الحقيقية لجرائم تقنية المعلومات هو «الأفعال الضارة وغير المشروعة كافة التي تلحق باقتصاد الدولة وأمنها الداخلي والخارجي وتشكل اعتداء على قيم المجتمع ومعتقداته وتلحق ضرراً مادياً أو معنوياً بالأفراد، إذا استخدمت في ارتكابها وسائل تقنية المعلومات أو وقع الاعتداء على المكونات المادية والمعنوية لهذه الوسائل ومخزوناتها، وكان مرتكبوها قد تعمدوا ارتكابها».

صلة التعريف بعنوان الدراسة والتسميات الأخرى:

في ضوء التعريف المقترح جاء اختيار الباحث لعنوان هذه الدراسة، حيث لاحظ أن قسماً «من الباحثين اختاروا الإطلاق على هذا النوع من الجرائم مسمى جرائم الحاسب الآلي والإنترنت، وآخرون أطلقوا عليها

مسمى الجرائم المعلوماتية أو الإلكترونية أو السيبرونية «Cyper Crimes»؛ ويقصد بهذه الأخيرة (جرائم الفضاء المعلوماتي).

ويرى الباحث أن تسمية جرائم الحاسب الآلي والإنترنت لا تخلو من القصور لربطها الجريمة بجهاز الحاسب الآلي فحسب، حيث أُخرج من دائرة التجريم الأفعال الضارة والانتهاكات التي تستخدم التقنيات الأخرى في مجال نظم معالجة البيانات والمعلومات وما يستحدث منها.

أما التسميات الأخرى فتنطوي على قدر كبير من التجاوز، نظراً لعمومية مصطلحات المعلوماتية والإلكترونية والسيبرونية والتي تتسم بالسعة والشمول، لذلك ينبغي تحديد هذا النوع من الجرائم في نطاق التقنيات المستخدمة في المجال المعلوماتي، وهو ما اتجه إليه المشرع في دولة الإمارات العربية المتحدة بصدور القانون الاتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، حيث أطلق على هذا النوع من الجرائم مسمى "جرائم تقنية المعلومات" معرفاً وسيلة تقنية المعلومات بأنها «أية أداة إلكترونية مغناطيسية بصرية كهروكيماوية أو أية أداة أخرى تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أية قدرة على تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة».[25]

فوفق هذا التعريف، فإن الوسيلة ومحل الجريمة ليست مقتصرة على جهاز الحاسب الآلي وشبكة الإنترنت فحسب، بل تشمل التقنيات كافة في

المجال المعلوماتي، كما أنها لا تتعلق بالمعلومات والإلكترونيات بحد ذاتها وإنما بتلك التي تندرج ضمن مظلة نظم تقنية المعلومات المعترف بها كنظام معلوماتي، في ضوء هذا المفهوم جاء استخدامنا لمصطلح جرائم تقنية المعلومات في عنوان هذه الدراسة.

ثانياً: تصنيف جرائم تقنية المعلومات وأنواعها

لا يوجد اتفاق على تصنيف محدد لجرائم تقنية المعلومات، سواء بين الباحثين أو التشريعات المتعلقة بهذا النوع من الجرائم. ويلاحظ أن اختلاف المفاهيم السائدة في المجتمعات وتنوعها قد ترك أثره على المنحى الذي اتخذه المشرعون والباحثون في تصنيفهم لجرائم تقنية المعلومات، إذ يتبين أن التشريعات الجزائية في الدول الغربية العلمانية قد ركزت جل اهتمامها على الانتهاكات التي تمس الجانب الاقتصادي والمالي والقرصنة وحقوق الملكية الفكرية، أما التشريعات المتعلقة بالانتهاكات الماسة بالجوانب العقائدية والأخلاقية فكانت نادرة؛ وهو ما يعكس الطبيعة العلمانية والثقافة التحررية لهذه المجتمعات.

وإضافة إلى ذلك، اتجه الباحثون العرب والمسلمون نحو التوسع في تجريم الانتهاكات الماسة بالمعتقدات الدينية والآداب العامة وحماية القيم الأسرية، وهو انعكاس لمفاهيم وثقافة خاصة تنتمي إليها مجتمعاتنا الشرقية التي توصف بالمحافظة والمختلفة عن المجتمعات الغربية التي توصف بالعلمانية.

1. التصنيفات القائمة على مفاهيم غربية (علمانية)

أ. التصنيف الأوربي:

في خطوة للتوصل إلى اتفاق تتحدد بموجبه أنواع جرائم تقنية المعلومات التي ينبغي ملاحقتها في الدول الأوربية، تبنى المجلس الأوربي الثالث والأربعون لسنة 2001 معاهدة حول الجرائم المرتبطة بالحاسب الآلي والإنترنت، تضمنت إجراءات التقاضي وصلاحيات قوات الشرطة في ملاحقة مرتكبي هذا النوع من الجرائم، حيث صنفت المعاهدة جرائم تقنية المعلومات من خلال أربع مجموعات كالآتي:[26]

المجموعة الأولى:

أ. الدخول غير القانوني.

ب. الاعتراض غير القانوني.

ج. تدمير المعطيات.

د. اعتراض النظم.

هـ. إساءة استخدام الأجهزة.

المجموعة الثانية: الجرائم المرتبطة بجهاز الحاسب الآلي:

أ. التزوير المرتبط بالحاسب الآلي.

ب. الاحتيال المرتبط بالحاسب الآلي.

المجموعة الثالثة: الجرائم المرتبطة بالمحتوى:

أ. الجرائم المتعلقة بالأفعال الإباحية للأطفال.

ب. الجرائم المتعلقة بالأفعال اللاأخلاقية.

المجموعة الرابعة: الجرائم المرتبطة بالإخلال بحق المؤلف:

أ. قرصنة البرمجيات.

ب. الاعتداء على حقوق الملكية الفكرية.

أثارت هذه المعاهدة الجدل لدى محاولتها حظر بعض النشاطات التي تستخدمها شبكة الإنترنت؛ مثل الدجل والاحتيال والصور الإباحية للأطفال، كما تعرضت لنقد شديد من نشطاء في مجال حقوق الإنسان جعلوا المعاهدة تعطي قوات الأمن سلطات إضافية، ولا تقدم الضمانات الكفيلة بحماية الحرية والخصوصية الشخصية في استخدام الإنترنت.[27]

ب. تصنيف وزارة العدل الأمريكية عام 2000:

حددت وزارة العدل الأمريكية أنواع جرائم الحاسب الآلي والإنترنت على النحو الآتي:[28]

1. السطو على بيانات الحاسب الآلي.
2. الاتجار بكلمة السر.
3. حقوق الطبع "البرامج وأفلام التسجيل الصوتي" وعمليات القرصنة.

4. سرقة الأسرار التجارية باستخدام الحاسب الآلي.

5. تزوير العملة باستخدام الحاسب الآلي.

6. الصور الجنسية الفاضحة واستغلال الأطفال.

7. الاحتيال بواسطة شبكة الإنترنت.

8. الإزعاج عن طريق شبكة الإنترنت.

9. تهديدات القنابل بواسطة شبكة الإنترنت.

10. الاتجار بالمتفجرات أو الأسلحة النارية أو المخدرات وغسل الأموال بواسطة شبكة الإنترنت.

ثم أضاف مكتب التحقيقات الفيدرالي الأمريكي "FBI"، إلى التصنيف السابق قائمة من سبعة أنواع من الجرائم صنفت على النحو التالي:[29]

1. اقتحام شبكات الهواتف العامة والخاصة بواسطة الحاسب الآلي.

2. اقتحام شبكة الحاسب الآلي الرئيسية لأي جهة.

3. انتهاك السرية لدى بعض المواقع بالإنترنت.

4. انتهاك سلامة الشبكة المعلوماتية.

5. التجسس الصناعي.

6. سرقة برامج الحاسب الآلي.

7. الجرائم الأخرى عندما يكون الحاسب الآلي العامل الرئيسي في ارتكاب المخالفات الجنائية.

ويلاحظ أن هذين التصنيفين لم يرد فيهما أي إشارة إلى الانتهاكات التي تمس المعتقدات الدينية والقيم الأسرية باستثناء الإشارة إلى الصور الفاضحة واستغلال الأطفال. وحتى هذا النص، تم نقضه بعد سنة من تطبيقه بناءً على قرار المحكمة العليا الأمريكية التي أصدرت حكمها بأغلبية خمسة قضاة مقابل أربعة بعدم دستورية هذا النص، واعتبرته انتهاكاً للتعديل الأول للدستور الأمريكي الخاص بحرية التعبير، وأضاف القرار أنه سيتاح للمحكمة مناقشة الوسائل الإلكترونية من أجل السماح للبالغين بشراء هذه المواد وفي الوقت نفسه الاحتفاظ بها بعيداً عن متناول الأطفال، وكان القانون يفرض غرامة قدرها 50 ألف دولار على من يضع مواد إباحية ضارة بالأحداث على شبكة الإنترنت يسهل الوصول إليها.[30]

هذا الأمر يعكس المفاهيم والمعتقدات السائدة في المجتمعات الغربية التي غالباً ما تتسامح مع هذا النوع من الانتهاكات.

2. التصنيفات القائمة على المفاهيم العربية والإسلامية

أ. تصنيف يونس عرب

في دراسته عن جرائم الكمبيوتر والإنترنت عام 2002، قسم الباحث يونس عرب جرائم الحاسب الآلي والإنترنت إلى أربع مجموعات وفق الآتي:[31]

1. التصنيف القائم على معطيات محل الجريمة، ويشمل الجرائم الآتية:

أ. الجرائم الماسة بقيمة معطيات الحاسب الآلي كجرائم الإتلاف والتشويه للبيانات والمعلومات والبرامج، وكذلك الجرائم الواقعة على ما تمثله المعطيات من أموال وأصول كجرائم غش الحاسب الآلي.

ب. الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة.

ج. الجرائم الماسة بحقوق الملكية الفكرية كبرامج الحاسب الآلي ونظمه كنسخ البرامج وتقليدها دون ترخيص.

2. تصنيف الجرائم تبعاً لدور الحاسب الآلي:

يقصد بذلك الجرائم الناجمة عن تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها، وهي تمثل المحتوى غير المشروع الذي يتم تخزينه في الحاسب الآلي، ويطلق على هذا النوع "جرائم التخزين"، حيث

يستخدم الحاسب الآلي لحفظ المواد المستخدمة في الجريمة أو المتحصلة عنها وتخزينها.

3. تصنيف الجرائم تبعاً للغرض النهائي أو المحل المستهدف:

يقوم هذا التصنيف على فكرة الغرض الجرمي المنوي تحقيقه أو الجهة المستهدفة في الاعتداء، ويشتمل هذا التصنيف على الجرائم الآتية:

أ. الجرائم الموجهة ضد الأشخاص، ويقصد بذلك الأفعال الجرمية التي تستهدف الأشخاص كجرائم القتل والإيذاء الجسماني الناجمة عن العبث أو التلاعب أو تخريب أجهزة الحاسب الآلي، وكذلك جرائم الإهمال والجرائم الجنسية والأخلاقية التي تتم من خلال الحاسب الآلي، وجرائم حض القصَّر على الأنشطة الجنسية وتحريضهم عليها أو إفسادهم عبر الوسائل الإلكترونية.

ب. جرائم الأموال المرتبطة بأنشطة اختراق البرامج أو إتلافها أو الاقتحام والدخول غير المشروع إلى نظام حاسب آلي أو شبكة الآخرين.

ج. جرائم الاحتيال والسرقة الناجمة عن التلاعب أو العبث بالمعطيات والنظم أو الحصول على بطاقات مالية للغير واستخدامها بدون موافقة أصحابها.

د. جرائم التزوير (كتزوير البريد الإلكتروني والوثائق والسجلات).

هـ. جرائم المقامرة والجرائم الموجهة ضد الأخلاق والآداب العامة، ومن أمثلتها (إدارة مشروع مقامرة على الإنترنت).

و. جرائم الحاسب الآلي الموجهة ضد الحكومة، ومن أمثلتها تعطيل الأعمال الحكومية أو الحصول على معلومات سرية، مهما كانت درجة سريتها.

4. الجرائم الواقعة على مكونات جهاز الحاسب الآلي والإنترنت:

وهي الأعمال الجرمية التي تستهدف المعلومات والبرامج المخزنة داخل الحاسب الآلي نفسه كسرقة مكونات أو أجزاء منها أو تخريبها، أما جرائم الإنترنت فهي تلك الناجمة عن الاعتداء على المواقع وتعطيلها أو تشويهها.

ب. تصنيف الدكتور محمد عبدالرحيم العلماء:

قسم الباحث محمد عبدالرحيم العلماء الجرائم المرتكبة عبر شبكة الإنترنت إلى ثماني مجموعات نعرضها على النحو الآتي:[32]

1. اختراق شبكات الحاسب الآلي وأجهزته المرتبطة بشبكة الإنترنت، ومن صوره:

أ. انتهاك المعلومات أو نسخها.

ب. اختراق الأنظمة عن طريق كسر مفتاح الأمان أو معرفة كلمة السر بطريقة غير مشروعة جاعلاً هذا النوع من أخطر أنواع جرائم تقنية المعلومات.

2. التجسس من خلال الاطلاع على المعلومات الخاصة بالغير المؤمَّنة في جهاز آخر، وليس مسموحاً لغير المخولين الاطلاع عليها؛ ومن صوره:

أ. التجسس العسكري.

ب. التجسس الصناعي.

ج. التجسس التجاري.

3. التخريب والإتلاف، ويقصد به التخريب الموجه إلى أجهزة الحاسب الآلي المرتبطة بشبكة الإنترنت؛ ومن صوره:

أ. مسح البيانات والبرامج المخزنة على الحاسب الآلي المستهدف.

ب. خلط وتشويش البيانات بجعلها غير صالحة للاستعمال.

ج. زرع فيروسات إلكترونية في جهاز الحاسب الآلي بواسطة البريد الإلكتروني.

4. التحريف والتزوير ومن صوره:

أ. التلاعب في المعلومات المخزنة في أجهزة الحاسب الآلي.

ب. اعتراض المعلومات المرسلة عبر أجهزة الحاسب الآلي عبر الشبكة الدولية بقصد تحريفها وتزويرها وتغييرها بهدف التضليل.

5. السرقة والاختلاس، ومن ذلك:

أ. سرقة معطيات الحاسب الآلي أو البيانات المخزنة.

ب. اختراق شبكات المصارف المالية والبنوك لإجراء تحويلات مصرفية غير مشروعة.

6. بث مواد لأفكار غير مشروعة عبر شبكة الإنترنت؛ ومن صوره:

أ. بث مواد وأفكار ذات خطر ديني.

ب. نشر مواد وأفكار ذات خطر أمني.

ج. بث مواد ذات خطورة على الأخلاق والعادات والقيم الاجتماعية.

7. إساءة استخدام البريد الإلكتروني، ومن صورها:

أ. تدمير معطيات الحاسب الآلي كلياً أو جزئياً.

ب. تبادل المواد المخلة بالآداب والعقيدة والأمن.

ويلاحظ أن هذين التصنيفين قد اتسما بالشمول وسعة التغطية للأفعال التي تنتمي لطائفة جرائم تقنية المعلومات كافة، وخاصة ما يتعلق منها بالانتهاكات الماسة بالقيم والآداب العامة والعقيدة الدينية، وهو ما يتماهى مع التوجه الفقهي المستند إلى المفاهيم العربية والإسلامية.

3. تصنيف جرائم تقنية المعلومات وفق قانون العقوبات الاتحادي رقم 2006/2

مع تسارع وتيرة تطور وسائل تقنية المعلومات ودخولها في نطاق الاستخدام اليومي لمعظم الأفراد كضرورة حياتية ووظيفية، تنبه المشرع بدولة الإمارات العربية المتحدة لأهمية وجود تشريع عقابي متقدم يعالج الإفرازات السلبية الناجمة عن الاستخدام غير المشروع لهذه التقنية الحديثة والمعقدة التي يريد العابثون حرفها عن مسارها بتحويلها من أداة تخدم ازدهار المجتمع وتطوره إلى أداة ضارة وخطرة تهدد أمن المجتمع وسلامة بنيانه الاقتصادي والاجتماعي.

وقد لاحظ المشرع بدولة الإمارات العربية المتحدة أن قانون العقوبات الاتحادي رقم 3 لسنة 1987 قاصر عن مواجهة هذا النوع من الجرائم، ولا يلبي الحاجة إلى تغطية أشكال جرائم تقنية المعلومات التي نشهدها اليوم وصورها كافة، باعتبار أن انتشارها كظاهرة جرمية على نطاق واسع كان لاحقاً لصدور ذلك القانون، ولمعالجة هذه المشكلة كان لابد من التحرك على المستوى التشريعي إما بتعديل قانون العقوبات أو إصدار قانون خاص على غرار القانون الخاص بالأحداث، يتصدى لهذه الظاهرة الجديدة على مجتمع الإمارات والضارة باقتصاده وقيمه ومعتقداته؛ فجاءت المعالجة بصدور القانون الاتحادي رقم 2/ 2006 بشأن مكافحة جرائم تقنية المعلومات الذي نشر بالجريدة الرسمية في كانون الثاني/ يناير 2006 ليعالج مشكلة النقص في التشريعات الجزائية بشقها الموضوعي.

تضمن قانون تقنية المعلومات الإماراتي 29 مادة، تتعلق بالأفعال الضارة والانتهاكات التي تستخدم فيها الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، حيث خصصت المادة الأولى للتعريف بالمصطلحات، أما المواد الأخرى فقد تضمنت تحديد الجرائم والعقوبات المقررة لكل منها.

ومما يجدر ذكره أن القانون جاء متناغماً مع المنهج القائم على المفاهيم العربية والإسلامية نحو التوسع في التصنيف؛ فشمل الجرائم الماسة بالعقيدة والآداب العامة، وشدد على الانتهاكات التي تمس القيم الإسلامية، أو نشر أخبار أو صور تتصل بحرمة الحياة الخاصة والعائلية وحدد عقوبتها بالحبس لمدة سنة وغرامة لا تقل عن خمسين ألف درهم، كما تضمن القانون تجريم مناهضة الدين الإسلامي وجرح الأسس والمبادئ التي يقوم عليها وحدد عقوبتها بالسجن مدة لا تزيد على سبع سنوات، بالإضافة إلى تجريم استخدام الوسائل التقنية في الاستيلاء على مال الغير أو تحويل الأموال بطريقة غير مشروعة، هذه التصنيفات وصورها سوف نتناولها بالتفصيل في ضوء نصوص هذا القانون وفق الآتي:

أولاً: الاعتداء العمدي على مواقع النظام المعلوماتي وتتضمن الصور التالية وفقاً للمادتين [2 و 3]:

أ. الدخول إلى النظام المعلوماتي بدون وجه حق أو تجاوز مدخل مصرح به.

ب. إلغاء البرامج أو حذفها أو تدميرها أو إنشاؤها أو إتلافها أو تغييرها أو إعادة نشرها، إذا تعلق الأمر ببيانات أو معلومات دون تصريح أو تخويل.

ثانياً: تزوير المستندات في النظام المعلوماتي، وتتضمن الصور التالية وفقاً للمادة [4]:

أ. تزوير مستندات الحكومة الاتحادية والمحلية.

ب. تزوير المستندات الأخرى إذا ترتب عليها ضرر.

ج. استخدام المستند المزور مع العلم بتزويره.

ثالثاً: إعاقة وسائل أو برامج تقنية المعلومات أو تعطيلها أو إتلافها أو مصادر البيانات بواسطة الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وتتضمن الصور الآتية وفقاً للمواد [5 و 6 و7]:

أ. الإيقاف عن العمل.

ب. التعطيل أو التزوير أو المسح أو الحذف.

ج. الإتلاف أو تعديل البرامج والبيانات أو المعلومات.

د. إتلاف الفحوص الطبية أو تشخيص العلاج.

رابعاً: اختراق السرية والتنصت والتقاط ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات عمداً وبدون وجه حق وفقاً للمادة [8]، ومن صورها:

أ. الدخول بقصد التنصت على مرسل غير مصرح به.

ب. الدخول بقصد التقاط مرسل غير مصرح به.

ج. الدخول إلى موقع بقصد إلغائه أو تغييره أو إتلافه أو الحصول عليه.

د. الدخول إلى موقع بقصد الحصول على معلومات حكومية سرية.

خامساً: استعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات وفقاً للمواد [9 و 10 و 11] بقصد:

أ. التهديد والابتزاز.

ب. الاستيلاء على مال منقول بطريق الاحتيال والخداع.[33]

ج. التوصل إلى أرقام وبيانات بطاقة ائتمانية أو بطاقة إلكترونية.

سادساً: استعمال الشبكة المعلوماتية أو وسائل تقنية المعلومات لبث أو إرسال ما من شأنه المساس بالآداب العامة والحض على الرذيلة والفجور وفقاً للمواد [12 و 13] ومن صورها:[34]

أ. إنتاج أو إعداد أو إرسال أو تخزين مواد بقصد الاستغلال والتوزيع من شأنها المساس بالآداب العامة أو إدارة مكان لذلك، وتشدد العقوبة إذا كانت موجهة لحدث.

ب. التحريض والإغواء لذكر أو أنثى على ارتكاب الدعارة أو الفجور، وتشدد العقوبة إذا كان المجني عليه حدثاً.

سابعاً: الاعتداء على موقع في الشبكة المعلوماتية بدون وجه وفقاً للمادة [14] بقصد، ومن صوره:

أ. تغير تصاميم الموقع.

ب. إلغاء الموقع أو إتلافه أو تعديله.

ج. شغل عنوان الموقع.

ثامناً: الإساءة للمقدسات والشعائر الدينية عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات وفقاً للمادة [15]، ومن صورها:

أ. الإساءة لأي من المقدسات والشعائر الدينية.

ب. الإساءة لأي من المقدسات والشعائر المقررة في الأديان الأخرى.

ج. سب أحد الأديان السماوية المعترف بها.

د. الحض على المعاصي والترويج لها.

هـ. مناهضة وجرح ما علم من الدين بالضرورة أو النيل منه.

و. التبشير أو الدعوة أو الترويج لدين أو فكر أو مذهب بما يسيء للدين الإسلامي.

تاسعاً: الاعتداء بواسطة الشبكة المعلوماتية على الحياة الخاصة وفقاً للمادة [16]، ومن صوره:

أ. نشر صور تتصل بحرمة الحياة الخاصة والعائلية.

ب. بث أخبار أو أقوال تتصل بحرمة الحياة الخاصة أو العائلية.

عاشراً: إنشاء المواقع أو نشر معلومات على الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات أواستخدامها لمقاصد جرمية وفقاً للمواد [17 و 18 و19 و 20 و 21]، ومن صوره:

أ. الاتجار بالبشر أو تسهيله.

ب. ترويج المخدرات أو المؤثرات العقلية وما في حكمها، وتسهيل التعامل بها.

ج. غسل الأموال أو تحويلها أو تمويه مصدرها.

د. تسهيل برامج وأفكار مخلة بالنظام العام أو بالآداب العامة وترويجها.

هـ. خدمة جماعة إرهابية أو تسهيل الاتصال بقيادتها أو أعضائها والترويج لأفكارها أو تمويلها.

و. تصنيع أجهزة حارقة أو متفجرة أو أية أدوات تستخدم لأعمال إرهابية.

حادي عشر: التحريض أو المساعدة أو الاتفاق على ارتكاب أي من الأفعال المنصوص عليها الواردة في هذا القانون بالمادة 23.

ويلاحظ أن قانون جرائم تقنية المعلومات الإماراتي قد تميز بقدر كبير من التوسع والشمول، بحيث غطى الأفعال والانتهاكات الضارة والخطرة كافة إذا استخدم في ارتكابها الشبكة المعلوماتية أو أي من وسائل تقنية المعلومات، مما يظهر أن المشرع قد أخذ بمعيار جمع فيه بين الوسيلة المستخدمة وموضوع الجريمة، سواء استخدم فيها جهاز الحاسب الآلي أو أي وسيلة من وسائل تقنية المعلومات؛ الأمر الذي يعطي القانون قدرة على استيعاب أي أفعال غير مشروعة تستخدم فيها ابتكارات مستقبلية في مجال تقنية المعلومات.

كما أن التحديد التفصيلي الذي أتى به القانون وشموليته يشير إلى حرص المشرع على تضمين الانتهاكات في مجال تقنية المعلومات جميعها ووضعها في دائرة التجريم، وخاصة ما ورد من نصوص تتعلق بالأفعال والانتهاكات الماسة بالأسرة والآداب العامة والمعتقدات الدينية والتعرض لرموزها، والذي جاء بلاشك تحت تأثير الانتشار الواسع وغير المقبول لهذا النوع من الانتهاكات التي تبث عبر الإنترنت ووسائل تقنية المعلومات التي أصبحت تشكل خطراً كبيراً على المجتمعات العربية والإسلامية وتسيء لمعتقداتها، وبذلك يكون القانون قد عالج واحداً من أهم التحديات التي كانت تواجه أجهزة التحقيق والعدالة الجنائية، بحيث وفر لها الركيزة التشريعية لمواجهة هذا النوع من الجرائم، بأن تم تمييز الأفعال المشروعة من غير المشروعة في مجال استخدامات الحاسب الآلي ونظم تقنية المعلومات.

التحقيق الجنائي في جرائم تقنية المعلومات

تقف أجهزة التحقيق والعدالة على خط الدفاع الأول في مواجهة ظاهرة الجريمة، وقد عملت هذه الأجهزة على تنمية قدراتها وتطوير إمكاناتها بصورة تواكب تطور أساليب الجريمة وتنوع أدواتها، وظلت هذه المواجهة سجالاً تخفق فيه السلطة أحياناً وتنجح في أحيان أخرى كثيرة، وكلما كانت الأجهزة المعنية بهذه المواجهة قادرة على التعرف على ظروف الجريمة وكشف ملابساتها وضبط أدلة إثباتها، أمسى النجاح حليفاً لها بإلحاقها الهزيمة بالجناة من خلال ضبطهم وجلبهم للعدالة.

إن تغيراً نوعياً قد حل في مسيرة هذه المواجهة بدأت معالمه تظهر مع التطور التكنولوجي المثير في مجال الاتصالات ونظم المعلومات في الثمانينيات من القرن الماضي، كان عنوانه جهاز الحاسب الآلي ثم شبكة الإنترنت فيما بعد؛ هاتان التقنيتان اللتان أصبحتا اليوم ضرورة حياتية ووظيفية للأفراد والمؤسسات والحكومات.

لقد وفرت هذه التطورات التكنولوجية التي تسارعت بشكل ملحوظ بيئة خصبة لبروز جرائم مستحدثة لا مثيل لها في الماضي؛ مما أوقع أجهزة التحقيق والعدالة الجنائية أمام تحد كبير ظهر فيه تفوق واضح لمرتكبي هذا النوع من الجرائم من حيث قدرتهم على التعامل مع هذه التقنيات الحديثة، والولوج إلى مكوناتها المعقدة، وتوجيهها نحو مقاصد جرمية لم تكن أجهزة التحقيق مستعدة لها، نظراً لافتقارها إلى الحد الأدنى من المعارف الفنية

والعملية الخاصة بهذه التقنيات، الأمر الذي يستوجب النهوض بمستوى هذه الأجهزة وتأهيل كوادرها بما يمكنهم من التعامل بكفاءة مع هذا النوع من الجرائم، وخاصة الإلمام بالجوانب الفنية المتعلقة بإجراءات جمع الاستدلالات والتحقيق الابتدائي.

أولاً: جمع الاستدلالات في جرائم تقنية المعلومات

تهيئ مرحلة جمع الاستدلالات التي يقوم بها رجال الضبط القضائي الطريق أمام مباشرة الدعوى الجزائية من قبل النيابة العامة التي تتولى عملية التحقيق بمعناها الواسع، ويلاحظ أن قانون الإجراءات الجزائية الإماراتي ومثله المصري قد أناط بمأموري الضبط القضائي مهمة تقصي الجرائم والبحث عن مرتكبيها وجمع المعلومات والأدلة اللازمة للتحقق والاتهام. هذه الإجراءات التي يخولها القانون لمأموري الضبط القضائي، الذين يقومون بها بعد وقوع الجريمة بصفتهم القضائية المقصودة بمرحلة الاستدلال، تختلف عن الإجراءات الإدارية المتمثلة في التدابير الوقائية والاحتياطات الأمنية التي ينفذها رجال الشرطة قبل وقوع الجريمة.[35]

هذه المهام والمسؤوليات المنوطة برجال الشرطة، سواء منها ما يهدف إلى منع الجريمة أو قمعها تنطبق على الجرائم التقليدية والمستحدثة على حد سواء، غير أن طبيعة الإجراءات المتخذة ووسائل تنفيذها والمهارات المطلوبة تختلف بين النوعين؛ فجرائم تقنية المعلومات تتطلب من رجال الضبط القضائي أن يكونوا على قدر معقول من الثقافة بطبيعة عمل الحاسب الآلي

ونظم تقنية المعلومات ليتمكنوا من مباشرة إجراءات جمع الاستدلالات، بحيث تتوافر لديهم المقدرة على فهم مضامين البلاغات واستيعاب معطيات مسرح الجريمة والتعامل مع أدلة الإثبات المتحصلة من الوسائل الإلكترونية، وسوف نتناول هذه الإجراءات من خلال:

1. البلاغ

عادة ما تظل الجريمة مستترة حتى يصل خبرها إلى السلطات العامة، ممثلة في جهة التحقيق المختصة.[36] هذا الوضع ينطبق على الجرائم كافة دون استثناء، لكنه يتجلى وضوحاً بالنسبة لجرائم تقنية المعلومات نظراً لطبيعتها، حيث يصعب على الأشخاص العاديين الإبلاغ عنها لما تتطلبه من مهارات فنية غير متوافرة سوى لفئات مهنية أو تخصصية في مجال الحاسب الآلي ونظم تقنية المعلومات، فلو أخذنا جريمة القتل أو السرقة أو التزوير في صورتها التقليدية مثالاً نجد أن أي شخص يمكنه الإبلاغ عن أي من هذه الجرائم إذا ما علم بها أو شاهدها.[37] لكن جريمة النصب والاحتيال أو التزوير وغيرها من جرائم تقنية المعلومات فليس بمقدور أي شخص الإبلاغ عنها ما لم تتوافر لديه المقدرة على التعامل مع جهاز الحاسب الآلي أو نظم تقنية المعلومات، ويستطيع إدراك الفعل غير المشروع من الفعل المشروع، وبالتالي إخبار السلطات المختصة بوقوعه.

وفي الأحوال جميعها، فإن أي بلاغ عن جريمة، سواء كان فاعلها مجهولاً أو معلوماً وتندرج تحت قانون جرائم تقنية المعلومات، فإن البلاغ ينبغي أن يتضمن العناصر الآتية:

1. تحديد مكان وقوع الجريمة:

على المبلغ تحديد المكان الذي وقعت فيه الأفعال غير المشروعة، ووصفها بما يسمح بالدلالة عليها كوصف موقع أو عنوان الشركة أو البنك أو المنزل الذي تعرض للاعتداء.

2. تحديد نوع الجريمة:

لا يكفي أن يقوم المبلغ بتحديد مكان وقوع الجريمة، بل ينبغي عليه أن يبين نوع الجريمة المرتكبة؛ ما إذا كانت اعتداءً على مال أو تزويراً أو مساساً بالقيم الدينية أو إخلالاً بالآداب العامة والقيم الأسرية.

3. تحديد محل الجريمة:

يجب على المبلغ أن يحدد لرجال الضبط القضائي المختصين الجهاز الذي وقعت عليه الجريمة والموقع الذي استهدفه الاعتداء.

تعد هذه العناصر مهمة وضرورية لمساعدة رجال الضبط القضائي في أي بلاغ متعلق بجرائم تقنية المعلومات، بحيث تمكنهم من تحديد معالم الجريمة ووضع خطة للتعامل معها من الناحيتين الفنية والقانونية.

ولا يشترط وجود صفة معينة للمبلغ، فالتبليغ حق لكل فرد من أفراد المجتمع، سواء كان له مصلحة في ذلك أو لا، بل يعد واجباً يفرضه القانون على كل شخص علم بوقوع جريمة إلا إذا كانت من النوع الذي يتطلب

شكوى وفق ما تنص عليه المادة 37 من قانون الإجراءات الجزائية الإماراتي.[38]

وليس بالضرورة أن يكون التبليغ عن جريمة وقعت بالفعل بل يجوز الإبلاغ عن أعمال تحضيرية أو عن جريمة في سبيلها للوقوع، في هذه الحالة فإن الإجراءات التي تتخذها السلطات العامة تعد من قبيل الإجراءات الاحترازية والوقائية وتهدف إلى منع وقوع الجريمة، ومن ثم فهي أعمال إدارية لا تندرج في إطار مرحلة الاستدلالات.

2. معاينة مسرح الجريمة

بعد تلقي البلاغ تأتي الخطوة الثانية وهي معاينة مسرح الجريمة والتي غالباً ما يقوم بها رجال الضبط القضائي للكشف على مكان وقوع الجريمة وفحصه والتحفظ على أي آثار أو مخلفات أو متعلقات مادية تمتُّ بصلة إلى الجريمة ومرتكبيها، وكذلك تصوير الموقع ووضع السيناريوهات المقترحة لكيفية حدوثها وزمن ارتكابها والملابسات المحيطة بها وإثباتها على مرتكبها.[39]

ويلاحظ أن معاينة مسرح الجريمة المعلوماتية ليس بالفائدة أو الأهمية التي يتمتع بها معاينة مسرح الجريمة التقليدية.[40] فالمعاينة بصورتها التقليدية تنحصر في البحث عن الأدلة المادية الملموسة، في حين أن الأثر الذي يتركه المجرم المعلوماتي غالباً ما يكون ذا طبيعة معنوية غير محسوسة يصعب التعامل معه عبر الوسائل التقليدية، فعمليات التزوير والاختلاس التي تقع

على المحررات الإلكترونية وبرامج الحاسبات الآلية لا تترك أثراً مادياً في محتواها وهناك صعوبة كبيرة في إثباتها، فأغلب البيانات والمعلومات التي يتم تداولها عبر الحاسبات الآلية ومن خلالها تجري العمليات الإلكترونية هي بطبيعتها رموز إلكترونية مخزنة على وسائط ممغنطة موجودة في ذاكرة الحاسب الآلي، ويصعب أن تخلّف وراءها آثاراً مرئية يستدل من خلالها على الجناة.[41]

كما أن مسرح الجريمة التقليدية محصور يمكن تحديده في نطاق جغرافي معين على عكس مسرح جريمة تقنية المعلومات الذي لا حدود له؛ لكونه يقع على شبكة الإنترنت المنتشرة في أنحاء العالم.

وعلى الرغم من قلة الفائدة المرجوة من معاينة مسرح جريمة تقنية المعلومات، وبخاصة أن اكتشافها عادة ما يتم بعد مرور وقت كفيل بتغيير آثارها إن وجدت، فيمكن استخدام الوسائل التقليدية في المعاينة بصورة تعود بالنفع على عملية التحقيق كتصوير جهاز الحاسب الآلي الذي تمت الأفعال الجرمية بواسطته أو وقعت على برامجه ومكوناته الداخلية، وكذلك يمكن رفع البصمات عن أجزاء الجهاز وملحقاته، وخاصة إذا كانت الجريمة المرتكبة من نوع التخريب أو الإتلاف، ولكن الأهم من ذلك كله يجب أن تقتصر المعاينة على الأشخاص الذين لديهم المقدرة والكفاءة الفنية في التعامل مع الحاسبات الآلية والشبكات ونظم المعلومات ممن تلقوا تدريبات في مجال التعامل مع مسرح جريمة تقنية المعلومات. هذه مسألة بديهية؛ لأن أي تعامل غير ذلك يمكن أن يؤدي إلى نتائج عكسية تعوق عملية التحقيق وتخرجها عن مسارها، لذلك ينبغي للقائمين على معاينة مسرح الجريمة مراعاة الإرشادات الفنية الآتية:

- التحفظ على الأجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الأشياء التي يعتقد أن صلة لها بالجريمة.

- إثبات الطريقة التي تم بواسطتها إعداد النظام والعمليات الإلكترونية، وخاصة ما تحتويه السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام،[42] وكذلك ملاحظة الرقم التعريفي للاتصال عبر الإنترنت المعروف بـ Internet Protocol الذي يرمز إليه بالرمز (IP) وهو معد لنقل البيانات من مكان إلى آخر عبر الإنترنت، ويعد حجر الزاوية في تبادل الاتصالات والمعلومات عبر الحاسبات والأجهزة المختلفة المرتبطة بشبكة الإنترنت، ويعد الرقم التعريفي بصمة المستخدم في الدخول إلى شبكة الإنترنت؛ كونه لا يتغير بالنسبة إلى مستخدم واحد في ذات الوقت والتاريخ، وبالكشف عنه يمكن تحديد رقم هاتف المتصل على شبكة الإنترنت وبالتالي تحديد مكانه بسهولة.[43]

- إثبات حالة التوصيلات والكبلات المتصلة بمكونات النظام كله؛ وذلك لإجراء مقارنة لدى عرض الأمر على القضاء.

- عدم نقل أي مادة متحفظ عليها من مسرح الجريمة قبل التأكد من خلو المحيط الخارجي بموقع الحاسب الآلي من أي مجالات لقوة مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة عليها.

- وضع الحراسة على المكان وعدم السماح لأي شخص من الاقتراب من الأجهزة ومكوناتها لحين الانتهاء من فحصها أو نقلها إلى الجهة المختصة إذا تطلب الأمر ذلك.

3. البحث والتحري

ربما يحالف الحظ رجال الضبط القضائي ويتم ضبط الفاعل في مسرح الجريمة أو تتوافر أدلة ومعلومات لكشف هويته منذ بدايات مرحلة الاستدلال، يحدث ذلك - في أغلب الأحيان - عندما يكون الفاعل أحد موظفي الشركة التي تعرضت للاعتداء فيتم ضبطه متلبساً أو بناءً على معلومات صادرة عن جهاز أمن الشركة أو عن طريق الصدفة. ونظراً للطبيعة الخاصة لجرائم تقنية المعلومات من حيث قدرة الجناة الفائقة على إخفاء أدلة الإثبات، وما يتميزون به من احتراف في التعامل مع التقنيات الحديثة في هذا المجال، وعدم تنبه المجني عليهم لوقوع الجريمة إلا بعد مرور وقت على ارتكابها، فغالباً ما يكون الفاعل مجهولاً أو معلوماً ولم يقبض عليه. في هذه الحالة، فإن الخطوة التالية التي ينبغي أن يتبعها رجال الضبط القضائي بعد معاينة مسرح الجريمة هي وضع خطة للبحث والتحري عن الفاعل أو الفاعلين وتحديد هويتهم وأماكن وجودهم وضبطهم وتقديمهم لجهة التحقيق، على أن يؤخذ في الاعتبار، في أثناء وضع الخطة، طبيعة الأدلة المستندة إلى المعالجة الإلكترونية للبيانات من حيث سهوله تدميرها، وإن كانت الجريمة التي يجري التحري بشأنها مستمرة من حيث نتائجها وتنفيذها،[44] ما يستوجب أن يكون المدى الزمني لتنفيذ الخطة قصيراً قدر الإمكان، لذلك يجب التركيز في هذه المرحلة على الجوانب التالية:

1. التثبت من حقيقة الجريمة ومقاصدها؛ فقد تكون الجريمة غير حقيقية أو أنها تهدف إلى إثارة البلبلة والإرباك أو صرف الأنظار عن جريمة أخرى وقعت أو في طريقها للوقوع.

2. التعرف على الأسلوب المتبع في ارتكاب الجريمة ومقارنته بالأساليب النمطية لبعض المتهمين يحصر الشبهات في دائرة ضيقة ويسهل عمل فريق البحث والتحري في كشف غموض الجريمة.

3. التأكد من الوسائل التقنية المستخدمة في ارتكاب الجريمة؛ الأمر الذي يساعد في حصر المشتبه بهم ضمن فئة معينة، ويسرِّع التعرف على الفاعلين.

4. وضع تصور عن الجاني أو الجناة المحتملين أو المشتبه بهم، بناء على ما تم جمعه من المعطيات السابقة.

ثانياً: إجراءات التحقيق في جرائم تقنية المعلومات

ما يميز إجراءات التحقيق عن إجراءات مرحلة جمع الاستدلالات التي تناولناها في المبحث السابق أن الأولى يترتب على إجرائها مساس بحرية الأشخاص وحرمة مساكنهم، لذلك أحاطها المشرع بضمانات قيدت حرية رجال الضبط القضائي في إجرائها واشترط عليهم الحصول على إذن سلطة التحقيق ممثلة بالنيابة العامة، وإلا عدَّ الإجراء باطلاً، باستثناء بعض الحالات كحالة التلبس.[45]

وتعد إجراءات التفتيش والضبط والتحقيق مع الأشخاص ذوي العلاقة من أعمال التحقيق التي أحاطها المشرع بهذه الضمانات، حيث نصت المادة 53 من قانون الإجراءات الجزائية الإماراتي على «أنه لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم بغير إذن كتابي من النيابة العامة، ما لم تكن الجريمة متلبساً بها وتتوفر أمارات قوية على أن المتهم يخفي في منزله أشياء أو أوراقاً تفيد كشف الحقيقة، ويتم تفتيش منزل المتهم وضبط الأشياء والأوراق على النحو المبين بهذا القانون».

كما أن المادة 47 من القانون نفسه أوجبت على مأموري الضبط القضائي سماع أقوال الأشخاص المقبوض عليهم أو المضبوطين ثم إرسالهم إلى النيابة العامة خلال مدة أقصاها 48 ساعة إذا لم يأتوا بما يبرئهم.

أما الإجراءات في مجال جرائم تقنية المعلومات فتتمثل في الآتي:

1. التفتيش

يعرِّف معظم فقهاء القانون الجنائي التفتيش بأنه إجراء من إجراءات التحقيق يقوم به موظف مختص بهدف البحث عن الأدلة المادية لجريمة وقعت بالفعل (جنائية أو جنحة) سواء كان ذلك لمكان له حرمة خاصة أو لشخص، من شأنه أن يفيد في كشف الحقيقة عن الجريمة ومرتكبها.[46]

وإذا كان التفتيش في إطار هذا المفهوم يستهدف العثور على الأدلة المادية لكشف الجريمة ومرتكبيها فإن السؤال يثور عن مدى إمكانية خضوع

الكيانات المعنوية للحاسبات الآلية ونظم تقنية المعلومات في مجال الجريمة المعلوماتية لهذا الإجراء.

للإجابة عن هذا السؤال يجب التفريق بين تفتيش الكيانات المادية للحاسب الآلي Hardware، وتفتيش البرامج والتطبيقات Software وما لها من شبكات اتصال خارجية، سواء على المستوى المحلي أو الدولي.

تفتيش المكونات المادية:

تخضع المكونات المادية لأجهزة الحاسب الآلي ونظم تقنية المعلومات للقواعد القانونية التقليدية الخاصة بالتفتيش، فليس هناك خلاف حول جواز تفتيشها كأي مكونات مادية للجرائم التقليدية.

إلا أن جواز تفتيش هذه المكونات يتوقف على طبيعة المكان الذي تتواجد فيه؛ فإذا كانت مكونات الجهاز منعزلة عن بعضها وممتدة إلى أجهزة بأماكن أخرى تتمتع بخصوصية كمسكن المتهم مثلاً بحيث تحتوي هذه الأجهزة على بيانات مخزنة أو برامج معلوماتية من شأن تفتيشها كشف الجريمة أو مرتكبها، فان جانباً من الفقه يرى أن إذن التفتيش الأصلي يجب أن يمتد إلى الأماكن الأخرى إذا توفر عاملان:[47]

الأول: إذا كان تفتيش الموقع الذي تمتد إليه هذه المكونات ضرورياً لكشف الحقيقة.

الثاني: إذا توافرت معلومات عن وجود مخاطر يخشى معها ضياع الأدلة.

أما بالنسبة لتفتيش المواقع التي لم يشملها إذن التفتيش الأصلي، فإنه لضرورات الاستعجال يمكن لعضو النيابة العامة إرسال إذن التفتيش بواسطة نظام الربط الإلكتروني المعتمد في المراسلات بين المؤسسات الحكومية في دولة الإمارات العربية المتحدة، ومن خلال البرنامج الجنائي الذي يربط مراكز وأقسام الشرطة بالنيابة العامة، وذلك تحقيقاً لعنصر السرعة والمباغتة التي تتطلبها عملية التفتيش في هذا النوع من الجرائم.

كما أنه من الثابت جواز التفتيش في حالات التلبس دون الحصول على إذن النيابة العامة، وفقاً لنص المادة 53 من قانون الإجراءات الجزائية الاتحادي رقم 35 لسنة 1992 «لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم بغير إذن كتابي من النيابة العامة ما لم تكن الجريمة متلبساً بها... إلخ».

لكن المشكلة تثور عندما تكون الأجهزة المطلوب تفتيشها موجودة خارج النطاق الإقليمي لجهة الاختصاص في الجريمة محل التحقيق، فإنه في هذه الحالة يستحيل اتخاذ إجراءات التفتيش على الحاسبات محل الجريمة؛ احتراماً لسيادة كل دولة على إقليمها، إلا إذا وجدت اتفاقيات بين الدولتين المعنيتين تسمح بمثل هذه الإجراءات، وهو الموضوع الذي سنتناوله لاحقاً في سياق الحديث عن التعاون الدولي.

أما بالنسبة لتفتيش الأشخاص الذين يعتقد حيازتهم لمكونات الحاسب الآلي أو مكونات مادية ذات صلة بجريمة تقنية المعلومات فإنه ينطبق عليهم الضمانات والقيود المنظمة لتفتيش الأشخاص فيما إذا تواجدوا في أماكن عامة أو خاصة.[48]

تفتيش المكونات المعنوية:

تثير جرائم تقنية المعلومات جدلاً فقهياً حول مدى خضوع الكيانات المعنوية للحاسب الآلي ونظم تقنية المعلومات لإجراء التفتيش، وقد اختلف الفقه القانوني في تقدير هذه الإمكانية، حيث يرى بعضهم أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فان المفهوم العام لكشف الحقيقة يمتد ليشمل البيانات الإلكترونية غير المحسوسة، بينما يرى آخرون عدم خضوع الكيانات غير المرئية أو غير المحسوسة لإجراء التفتيش ما لم تعدَّل التشريعات القانونية بما يسمح باستيعاب هذه التطورات التكنولوجية، بحيث تشمل جميع الأدلة المادية والمعنوية.[49]

والحقيقة أن معيار جواز التفتيش على المكونات المعنوية من عدمه يعود للنصوص القانونية المتعلقة بالإجراءات الجزائية لكل دولة، حيث يلاحظ أن العديد من الدول تضمنت قوانينها نصوصاً تتحدث عن تفتيش الأشياء المتعلقة بالجريمة، وتؤدي إلى الكشف عنها وعن مرتكبيها، في هذا المعنى نصت المادة 251 من قانون الإجراءات الجنائية اليوناني أن «السلطات التحقيق صلاحية القيام بأي شي يكون ضرورياً لجمع الدليل وحمايته»؛ فهذا

النص يشمل جمع المكونات المادية وغير المادية المتعلقة بالجريمة مادام ضبطها يؤدى إلى الكشف عن الأدلة وتعزيزها، وينسحب على المكونات المعنوية المخزنة في ذاكرة الحاسب الآلي أو المعالجة إلكترونياً.[50]

وجاء في ذات المعنى ما نصت عليه المادة 487 من القانون الجنائي الكندي بأن «صلاحية إصدار إذن التفتيش تمتد إلى أي شيء مادامت توفرت أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو هناك شبهة في ارتكابها مع وجود نية أن تستخدم في ارتكاب الجريمة».[51]

ويذكر أن قانون الإجراءات الجزائية الاتحادي الإماراتي رقم 87 لسنة 1992 قد أكد المفهوم نفسه، حيث أشارت نصوص المواد (51،53،55،57) من هذا القانون إلى أن التفتيش يقع على الأشياء المتعلقة بالجريمة أو التي تكون لازمة للتحقيق فيها، وقد تكررت كلمة أشياء في هذه المواد جميعها دون أن تحدد ماهية هذه الأشياء، إن كانت مادية أو معنوية.[52]

فوفقاً لهذه النصوص، فإن المشرِّع في دولة الإمارات العربية المتحدة قد ترك الباب مفتوحاً لإمكانية تفتيش الكيانات المعنوية على غرار الكيانات المادية، ضمن ضوابط ينبغي مراعاتها عند إجراء التفتيش على هذه الكيانات، وهي لا تختلف عن القواعد التي تحكم الجرائم التقليدية التي يشترطها القانون، وهي كالآتي:

1. لإجراء التفتيش في جرائم تقنية المعلومات بمعناه القانوني يجب أن تكون الجريمة قد وقعت بالفعل، وأن الفعل المرتكب قد تم تجريمه

وفق نصوص قانون تقنية المعلومات الاتحادي رقم 2/ 2006 تأكيداً لمشروعية التفتيش.

2. أن تتوافر أمارات قوية تفيد بوجود أشياء؛ كالأجهزة أو المعدات أو المدخلات أو النظم أو البرامج تتعلق بالجريمة، وتفيد في كشف الحقيقة أو أنها لازمة للتحقيق.[53]

3. إذا كان محل التفتيش شخصاً معيناً أو أكثر، فإنه يجب توافر دلائل كافية تدعو للاعتقاد بوجود صلة له/ لهم بالجريمة، وأن التفتيش يفيد في كشف الجريمة أو مرتكبيها.[54]

4. خضوع مكونات الحاسب الآلي كافة ونظم تقنية المعلومات ذات الصلة بالجريمة للتفتيش بنوعيه المادي والمعنوي، من حيث وحدات الإدخال والإخراج والذاكرة والتخزين والكيانات المنطقية؛ كالبرامج والنظم والسجلات.[55]

5. أن ينفذ التفتيش بمعرفة خبراء في مجال الحاسب الآلي ونظم تقنية المعلومات أو من رجال الضبط القضائي ممن تلقوا تدريبات على هذا النوع من التفتيش الذي يتطلب مهارات فنية خاصة.

6. أن يقتصر التفتيش على الأشياء التي تفيد في كشف الجريمة ومرتكبيها، ولا يجوز تعمد البحث عن جريمة أخرى إلا إذا ظهرت عرضاً في أثناء التفتيش.

نخلص من هذا إلى أن التفتيش المتعلق بجرائم تقنية المعلومات يجب أن يشمل مكونات الجريمة ومتعلقاتها المادية والمعنوية كافة، وفق نصوص قانون الاجراءات الجزائية لدولة الإمارات العربية المتحدة في حدود الضوابط المقررة في هذا القانون.

2. الضبط

الغاية من التفتيش هي ضبط كل ما يفيد في كشف الحقيقة، سواء تعلق ذلك بأشخاص أو أماكن أو أشياء طالما كان لها اتصال بالجريمة.[56] والضبط يعني قيام السلطات المختصة بالتحفظ على متعلقات الجريمة بما يفيد الكشف عنها أو عن مرتكبيها. وإجراء الضبط ذو طبيعة مزدوجة؛ فقد يكون جزءاً من مرحلة التحقيق أو مرحلة الاستدلال، فإذا تطلب الأمر نزع حيازة الشيء بواسطة الجبر أو الاعتداء، فإن الإجراء في هذه الحالة يكون جزءاً من مرحلة التحقيق، أما إذا لم يتطلب الأمر ذلك، فيعد جزءاً من مرحلة الاستدلال.[57]

محل الضبط

ينسحب إجراء الضبط على الأشياء بصرف النظر عن موقع وجودها، فقد تكون في مكان أو بحوزة شخص، ويقع الضبط على المنقول والعقار، ويستوي أن تكون الأشياء محل الضبط مملوكة للمتهم أو لغيره، والأصل أن إجراء الضبط لا يقع إلا على الأشياء المادية غير أن التطورات التقنية المتسارعة واستخداماتها الواسعة قد فرضت تفسيراً منطقياً للنصوص

القانونية بما يسمح بخضوع المكونات المادية والمعنوية جميعها لهذه التقنيات لإجراء التفتيش والضبط.[58]

لقد أعيد إنتاج الخلاف الفقهي الذي أثير حول إجراء التفتيش ومدى خضوع المكونات المعنوية لوسائل تقنية المعلومات لهذا الإجراء الذي تناولناه في حديثنا عن التفتيش في المطلب السابق، حيث تبين أن التشريعات الجزائية قد فسحت المجال أمام جوازه على المكونات المعنوية كون لفظ الأشياء يمتد مدلولها إلى كل ما يفيد في كشف الحقيقة سواء كان ذا طبيعة مادية أو معنوية، هذا ينطبق على إجراء الضبط الذي هو غاية التفتيش ومبتغاه، كما أن الكيانات المعنوية كالبيانات المعالجة إلكترونياً المكونة من ذبذبات إلكترونية أو موجات كهرومغناطيسية أو المعلومات المخزنة، جميعها تقبل التسجيل والحفظ على وسائط مادية كالأقراص والشرائط الممغنطة، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها؛ وبذلك يمكن أن تخضع لإجراء الضبط والتحفظ عليها من خلال هذه الوسائط.[59]

وبناءً عليه، فإن الأشياء التي ينبغي إخضاعها لإجراء الضبط في جرائم تقنية المعلومات والتي تعد كيانات ذات قيمة يمكن الاستفادة منها في إثبات الجريمة أو نسبتها إلى الجاني هي:

1. وحدة المدخلات المكونة من مفردات لوحة المفاتيح Keyboard، والشاشة Monitor، والفأرة Mouse، والخادم Server؛ مجمع المعلومات، والماسحة الضوئية Scanner، وكذلك برنامج معالجة النصوص Word، وبرنامج عرض الشرائح PowerPoint.[60]

2. ضبط المستندات والكيانات الورقية التي وقعت عليها العمليات الإلكترونية والتي يعتقد أن لها صلة بالجريمة أو مرتكبيها، وقد تكون محررات مزورة داخل نظام الحاسب الآلي أو في أي مكان خارجه، ويمكن أن تكون في سلة المهملات.[61]

3. ضبط وحدة الذاكرة الرئيسية، ووحدة التحكم، والمودم (وهي الوسيلة التي تتمكن من خلالها أجهزة الحاسوب من الاتصال فيما بينها بواسطة خطوط الهاتف).[62]

4. الشرائط المغنطة؛ وهي جميع الشرائط ووسائط النقل والتخزين التي يعتقد أنها تحتوي على مواد تفيد في كشف الحقيقة أو مرتكبيها.

5. ضبط الطابعات وأجهزة التصوير بكافة أنواعها، ولاسيما أن الأجهزة الحديثة يمكنها تخزين المستندات والمواد المطبوعة أو المنسوخة، حيث يمكن إعادة استخراجها والتعرف على محتوياتها.

6. ضبط المراسلات الإلكترونية التي تستخدم البريد الإلكتروني عبر شبكة الإنترنت والتي يتم من خلالها نقل الرسائل ومحتوى المستندات الورقية، حيث تتمتع هذه الوسيلة بنظام حماية تتكون من رموز وشفرات لا يمكن الاطلاع عليها إلا إذا تعرفت عليها الجهة المستقبلة، وهي تحتفظ بنسخ عن المواد المرسلة منها وإليها يمكن استرجاعها والاطلاع عليها وضبطها.[63]

إن ضبط المعلومات يواجه صعوبات كبيرة عندما تكون هذه الأدلة متصلة بنظام يمتد خارج النطاق الإقليمي للدولة التي تقوم بالتحقيق في الجريمة؛ الأمر الذي يتطلب تعاوناً دولياً لإضفاء المشروعية على عملية الضبط.[64]

ونشير إلى ما سبق ذكره في موضوع التفتيش، وهو ضرورة أن يتولى إجراء الضبط أشخاص مؤهلون قادرون على التعامل مع متعلقات جريمة تقنية المعلومات بكفاءة، بحيث يكونون على دراية بالوسائل المستخدمة ووظائفها وحفظها على شرائط لاستخدامها كأدلة في مواجهة الجاني أمام الجهات القضائية.

3. التحقيق مع الأشخاص

تستمد عملية التحقيق مع الأشخاص زخمها وفقاً للمعطيات التي توصل إليها المحقق من خلال الإجراءات السابقة التي عرضناها في مرحلتي الاستدلال والتحقيق مجتمعة، بحيث يضع أمامه سجل الأدلة والقرائن التي جمعت بشأن الجريمة، بوصفها الأساس الذي تقوم عليه خطة التحقيق مع الأشخاص ذوي العلاقة بالجريمة، فكلما كانت الأدلة والقرائن التي بين يدي المحقق حاسمة وقوية سهل ذلك وصول عملية التحقيق إلى مرادها بالكشف عن المتورطين وإحالتهم إلى القضاء لينالوا جزاء أفعالهم، أما إذا كانت الأسس القائمة لدى المحقق ضعيفة وغير مترابطة، فإن العملية برمتها تكون عرضة للانهيار ولن تؤدي إلى شيء سوى تبديد الجهد وهدر الوقت.

والتحقيق الذي نعنيه في هذا المجال يتسع لسؤال الأشخاص ذوي العلاقة بجريمة تقنية المعلومات كافة وتدوين أقوالهم؛ وهو يشمل المشتبه بهم، واستجواب المتهمين، وسؤال شهود الإثبات والنفي، ومواجهة المتهمين بالأدلة التي بحوزة المحققين، وإجراء المواجهة فيما بينهم وكذلك مع الشهود، واصطحابهم إلى مسرح الجريمة للتثبت من أقوالهم وتحديد أدوارهم.

وللقيام بهذه المهام في مجال جرائم تقنية المعلومات، فإنه يتطلب من القائمين على التحقيق معرفة الجوانب التقنية والمصطلحات العلمية الخاصة بالوسائل والأجهزة المستخدمة في مجال تقنية المعلومات ونظمها، ليتمكنوا من السير بعملية التحقيق إلى هدفها.

ونظراً لطبيعة هذا النوع من الجرائم، وعدم قدرة أجهزة التحقيق على مجاراة تطورها المتسارع، خرجت فكرة مفادها إسناد مهمة التحقيق في هذه الجرائم إلى بيوت خبرة متخصصة في مجال الحاسب الآلي ونظم تقنية المعلومات؛ وذلك لسد النقص الذي تعانيه سلطات التحقيق وأجهزة العدالة الجنائية،بحيث يتم إيجاد نوع من التوازن في معادلة الصراع بين أجهزة السلطة والمجرم المعلوماتي التي تميل حالياً لصالح الأخير.[65]

هذه الفكرة وإن كانت جديرة بالبحث، إلا أنها تحتاج إلى توضيح مدى السلطات التي سوف تتمتع بها بيوت الخبرة والصلاحيات التي تخول لها في مجالات عملية التحقيق المختلفة، التي يخشى منها أن تكون على حساب

سلطات التحقيق وأجهزة العدالة الجنائية الرسمية المعنية أساساً بصيانة حقوق المجتمع، بعيداً عن المنافع والمكاسب المادية التي تسعى بيوت الخبرة لتحقيقها،[66] كما أن بعض جرائم تقنية المعلومات تمس أمن الدول ومصالحها العليا؛ مما يشكل خطراً استراتيجياً يتمثل في اطلاع بيوت الخبرة على أسرار الدولة وأجهزتها الحساسة فتكون عرضة للتداول والوقوع في أيدي أجهزة دول أو منظمات معادية. ولتجاوز هذه الإشكالية ينبغي الجمع بين المعرفة التقنية والعملية المتوافرة لدى خبراء أجهزة الحاسب الآلي ونظم تقنية المعلومات من جهة، وبين المعرفة المهنية والقانونية التي تتمتع بها أجهزة التحقيق الجنائي من جهة أخرى، ولتحقيق هذه الغاية لابد من إيجاد الآلية المناسبة ضمن هيكلية إدارية تستوعب هذا النوع من التعاون الفريد وغير المسبوق بين سلطات التحقيق وأجهزة العدالة الجنائية من جانب، وبين خبراء في مجال الحاسب الآلي ونظم تقنية المعلومات من جانب آخر، يمثلون القطاع الخاص في واحدة من المجالات السيادية الحساسة، والتي طالما جعلتها الدولة حكراً عليها لما تمثله من أهمية لأمنها الداخلي واستقرار بنيانها الاجتماعي.

ثالثاً: وسائل دعم مرحلة التحقيق في جرائم تقنية المعلومات

فرضت الطبيعة الخاصة لجرائم تقنية المعلومات على جهات التحقيق آليات عمل لم تكن تحتاج إليها من قبل، فنقص الخبرة وقلة المعرفة التقنية في مجال الحاسب الآلي ونظم تقنية المعلومات وضع المحققين أمام خيار الاستعانة بالخبراء في هذا المجال حتى يتمكنوا من التعامل مع هذا النوع من

الجرائم وفهم معطياتها، ويلاحظ أن هذا الشكل من التعاون يختلف عنه في الجرائم الأخرى المعتادة؛ إذ إنه يتطلب من الخبير في مجال الحاسب الآلي ونظم تقنية المعلومات التعاون مع المحقق في عملية التحقيق برمتها، حيث لا يقتصر ذلك على مجال معين من مجالات الخبرة المهنية التخصصية، كما هو الحال بالنسبة للجرائم التقليدية المعتادة كالطبيب الشرعي أو خبير البصمة، بل يقتضي الأمر وقوف الخبير على المفاصل الأساسية لعملية التحقيق، لذلك ينبغي استحداث آلية تضمن التعاون الفعال والمفيد في هذا المجال.

1. الاستعانة بالخبراء في مجال جرائم تقنية المعلومات

عندما يعجز المحقق أثناء التحقيق في جريمة ما عن فهم الجوانب التقنية أو العلمية التي تحتاج إلى قدر متقدم من التخصص لكشف غموضها أو فهم طبيعتها، أجاز له القانون الاستعانة بأشخاص أو جهات فنية أو مخبرية أو مهنية متخصصة في المسألة موضوع الخبرة.[67] وتعد الاستعانة بالخبراء جزءاً من عملية التحقيق، يقوم بها محقق الشرطة في مرحلة الاستدلال وعضو النيابة العامة في مرحلة التحقيق أو القاضي في مرحلة المحاكمة، وذلك للمساعدة في كشف غموض الجريمة وإثبات أدلتها في مواجهة الجناة أو المشتبه بهم أو نفيها عنهم؛ لأن نفي الاتهام لا يقل أهمية في ميزان العدالة عن إثباتها، ومن أمثلة ذلك الاستعانة بالطب الشرعي لتحديد سبب الوفاة ووقتها ونوع الأداة وطريقة استخدامها، أو الاستعانة بخبير البصمة لرفع البصمات أو المختبر الجنائي لإجراء الفحوص البيولوجية على العينات المضبوطة.

وإذا كانت الاستعانة بالخبير في بعض الجرائم مسألة تقديرية يترك شأنها للجهة القائمة على التحقيق أو المحاكمة،[68] وهو ما عبرت عنه المادة 40 من قانون الإجراءات الجزائية الإماراتي، التي نصت على «لمأموري الضبط القضائي أثناء جمع الأدلة أن يسمعوا أقوال من تكون لديهم معلومات عن الوقائع الجنائية ومرتكبيها وأن يسألوا المتهم عن ذلك ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة... »، فإن الأمر يختلف إذا كان موضوع الفحص يتعلق بمسائل فنية أو علمية بحتة؛ ففي هذه الحالة يصبح لزاماً على سلطة التحقيق الاستعانة بالخبراء والمختصين، لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه دون أن تتوافر لديه المعارف اللازمة يجعل حكمه معيباً يضر بمصلحة التحقيق ويعوق الوصول إلى الحقيقة. وقد أشارت المادة 96 من قانون الإجراءات الجزائية الإماراتي إلى أنه «إذا اقتضى التحقيق الاستعانة بطبيب أو غيره من الخبراء لإثبات حالة من الحالات كان لعضو النيابة العامة أن يصدر أمراً بندبه ليقدم تقريراً عن المهمة التي يكلف بها».[69]

فالمسألة تتعلق - كما تشير هذه المادة - بمقتضيات التحقيق وضرورات إثبات الحالة في الجريمة المرتكبة، ومن الواضح أنه ليست هناك جرائم أحوج إلى تدخل الخبراء من جرائم تقنية المعلومات التي تتميز بطبيعتها الفنية المعقدة وتمتعها بخاصية التطور المتسارع والمتلاحق الذي يتطلب درجة عالية من التخصص والقدرات الفنية المتميزة، وهذا ما تفتقر إليه جهات التحقيق في المجالات التي تتطلبها عملية التحقيق في هذا النوع من الجرائم؛ بدءاً من تلقي البلاغ، ومروراً بالبحث والتحري ومعاينة مسرح الجريمة والتفتيش والضبط، وانتهاء بالتحقيق مع الأشخاص المتورطين واستجوابهم.

إن اختيار الخبير في جرائم تقنية المعلومات يتوقف على نوع الجريمة المرتكبة ومجال الخبرة المطلوبة وطبيعتها الفنية. فلا يكفي حصول الخبير على درجة علمية معينة، وإنما ينبغي أن تكون لديه خبرة عملية تخصصية وكفاءة فنية عالية في حقل أو أكثر من حقول تقنية المعلومات ونظمها ووسائلها؛ فقد تكون الجريمة المرتكبة تزوير مستندات، أو تلاعباً في البيانات، أو الغش أثناء نقل أو بث البيانات، أو إطلاق الفيروسات أو قرصنة أو اعتداءً على حرمة الحياة الخاصة، أو التجسس.[70] كل هذه الجرائم تحتاج إلى مجالات متنوعة من الخبرة نعرض فيما يلي بعض نماذجها:

1. أن يكون الخبير متخصصاً في مجال تركيب المكونات المادية للحاسب الآلي وأنواعها ومصادر صناعتها وملحقاتها من الأجهزة.

2. أن تتوافر لديه الخبرة المتميزة في مجال النظم والبرامج والشبكات والمعالجة الآلية وكلمات المرور والسر ونظم التشفير.

3. أن تتوافر لديه القدرة على تحويل أدلة الإثبات من الكيانات غير المحسوسة إلى كيانات مقروءة أو مرئية وعزل النظام المعلوماتي، دون إلحاق أي هدر بالأدلة المستهدفة.

4. القدرة على تتبع مصادر الاعتداء وتحركات مستخدمي الحاسب الآلي، من حيث المعلومات التي يقدمونها والمواقع التي يزورونها ومشاركاتهم في المنتديات وغرف الدردشة والرسائل والصور التي يبثونها.

2. اقتراح استحداث وحدات تحقيق متخصصة في جرائم تقنية المعلومات

أ. فكرة الاقتراح:

تتمحور فكرة هذا الاقتراح حول استحداث وحدات أو فروع ضمن الهيكل التنظيمي لمراكز وأقسام التحقيق الرئيسية التي تخدم التجمعات الحضرية تختص بالتعامل مع جرائم تقنية المعلومات بأنواعها كافة ضمن النطاق الجغرافي لاختصاص المركز، على أن ترفد بكادر وظيفي من الضبطية القضائية ممن لديهم القابلية والقدرة على التكيف مع الأبعاد الفنية والعلمية لجرائم تقنية المعلومات، ويخولون صلاحيات الاستعانة بالخبراء المتخصصين في مجال الحاسب الآلي ونظم تقنية المعلومات، ضمن خطة ثلاثية أو خمسية يخضع فيها فريق العمل لبرامج تدريب وتأهيل، ويتم خلالها بصورة متدرجة في المدى الزمني المحدد للخطة، التقليل التدريجي من الاعتماد على خدمات الخبراء، بحيث تصبح هذه الوحدات في نهاية المدة، قادرة على التعامل بكفاءة وفاعلية مع متطلبات عملية التحقيق الجنائي في جرائم تقنية المعلومات كافة.

ب. آلية عمل الوحدات المستحدثة في التعامل مع جرائم تقنية المعلومات:

1. تستقبل الوحدات المتخصصة البلاغات المعتبرة من جرائم تقنية المعلومات، بحيث يتولى المحقق سماع أقوال المبلغ وتدوينها وطلب المستندات والأوراق والمواد ذات العلاقة وإرفاقها بمحضر الاستدلال.

2. يستدعى الخبير إلى المركز و يطلع على محضر الاستدلال وما تضمنه من أقوال المبلغ والمستندات والمواد المرفقة ويتبادل المعلومات مع المحقق

حول الواقعة وتصنيفها والإجراءات اللازمة التي ينبغي اتخاذها وبيان مصطلحاتها.

3. بعد تدارس المعطيات المتوافرة في البلاغ يقوم المحقق المختص بالانتقال إلى مسرح الجريمة للمعاينة وإجراء مقابلات استطلاعية مع ممثلي الجهة التي تعرضت للاعتداء بحضور الخبير.[71] وعلى المحقق في هذه المرحلة أن يثبت ما يلي:

أ. جدية البلاغ ووقوع الجريمة.

ب. نوع الجريمة وطبيعتها.

ج. الأسلوب التقني المستخدم في ارتكاب الجريمة.

د. تحديد دوافع الجريمة.

هـ. تحديد الشهود.

و. تحديد المتهمين أو من هم في دائرة الشبهة.

4. بعد التثبت من النقاط السابقة يقوم المحقق، بناء على خبرته المهنية، بتصنيف الأشخاص ذوي الصلة بالجريمة إلى ثلاث فئات: شهود، ومشتبه بهم، ومتهمون، ثم يبحث في سجلاتهم الجنائية للتأكد إن كانت لهم سوابق أم لا.

5. يقوم المحقق بالتعاون مع الخبير بإعداد ملف الأدلة المتحصلة من معاينة مسرح الجريمة وما أسفر عنه التفتيش من مضبوطات وفرز المعلومات

المتوافرة من قبل التحريات والمصادر الأخرى للبدء في عملية سؤال الأشخاص والتحقيق مع المتهمين.

6. سؤال شهود الواقعة بحضور الخبير مع التركيز على ما لديهم من معلومات أو أدلة أو قرائن قد تقود إلى اتهام أشخاص محددين.

7. التحقيق مع المتهمين ومواجهتهم بالأدلة والقرائن وشهود الإثبات بحضور الخبير. وفي هذه المرحلة يستثمر المحقق خبراته المهنية ومواهبه الشخصية، وذلك من خلال الآتي:

   أ. طريقة طرحه للأسئلة.

   ب. قدرته على التأثير باستخدام لغة الجسد.

   ج. قدرته على قراءة ردود الفعل والانفعالات التي تصدر عن الطرف الآخر.

   د. موهبته في كسب ثقة الخاضعين للتحقيق.

أما الخبير فدوره يقتصر في هذه المرحلة على المراقبة والتدخل في المسائل التقنية عند الحاجة إلى التوضيح أو التصحيح، وله أن يسهم مع المحقق في إعداد الأسئلة أو التنبيه لموضوع ما من خلال ورقة يقدمها إلى المحقق.

مع انتهاء التحقيق مع المتهمين أو المشتبه فيهم تكون مهمة الخبير في هذه المرحلة قد انتهت، ويواصل المحقق إجراءاته الإدارية المتعلقة بإحالة الواقعة إلى جهة الاختصاص.

ج. محاذير ينبغي التنبه لها أثناء التحقيق:

نشير هنا إلى بعض المحاذير التي ينبغي التنبه لها أثناء التحقيق والتي تفرضها خصوصية هذا النوع من الجرائم، وتتمثل فيما يأتي:

1. إن الأدلة المستندة إلى المعالجة الآلية للبيانات يمكن التخلص منها بسرعة فائقة وهي متاحة للمحقق في زمن قصير؛ لذلك ينبغي عليه التصرف بسرعة لضمان سلامتها والحفاظ عليها أو نقلها إلى مكان آخر.

2. إن الجريمة المرتكبة قد تكون من الجرائم المستمرة التي ماتزال تنتج أثرها أو أنها ستار لجريمة أخرى، فعلى المحقق، بالتعاون مع الخبير، العمل بسرعة للتعرف على دوافع الاعتداء ومصادره والبرامج المستخدمة.

3. قد تتعرض البيانات والأدلة لمحاولة تدخل بهدف تدمير الأدلة أو تضليل التحقيق أو إعاقته.

4. قد يكون من بين الشهود متهمون أو مشتبه بهم.

د. الأهداف المتوخاة من استحداث وحدة مكافحة جرائم تقنية المعلومات:

استحداث وحدة التحقيق في جرائم تقنية المعلومات ضمن الهيكل التنظيمي لمراكز وأقسام الشرطة يحقق أهدافاً عديدة؛ نجملها فيما يأتي:

1. إسناد عملية التحقيق في جرائم تقنية المعلومات لجهة متخصصة يخفف العبء عن جهاز التحقيق المثقل بأعباء الجريمة التقليدية.

2. قيام جهة متخصصة بالتعامل مع جرائم تقنية المعلومات يضمن تحقيق قدر أكبر من الكفاءة والفاعلية في الأداء؛ الأمر الذي سوف يسهم في الحد من هذه الجرائم.

3. توفير بيئة عمل مناسبة لضمان تعاون مثمر بين المحقق والخبير، بعيداً عن زحمة العمل بالجرائم الأخرى والمراجعين.

4. استيعاب الكوادر المتميزة القادرة على التكيف مع التقنيات الحديثة واستخداماتها، وتوفير بيئة عمل تستجيب لملكاتهم وتوجهاتهم؛ مما ينعكس إيجابياً على أدائهم وانتمائهم الوظيفي.

5. استحداث الوحدة المتخصصة سيؤدي إلى سهولة تحديد برامج التدريب والتطوير في مجالات جريمة تقنية المعلومات وتحسين مخرجاتها.

6. خفض المدى الزمني الذي تحتاج إليه أجهزة التحقيق الجنائي للاستغناء عن خدمات الخبراء أو تقليل الاعتماد عليهم.

والحقيقة أن تدخل الخبراء على النحو الذي تتطلبه عملية التحقيق في جرائم تقنية المعلومات يحمل الكثير من السلبيات والمخاطر، لذلك ينبغي على أجهزة التحقيق والعدالة الجنائية أن تضع في حسبانها أن الاستعانة

بالخبراء مسألة اقتضتها الضرورة، وهي حالة مؤقتة يجب أن تنتهي، لذلك عليهم اتباع استراتيجية للتطوير والتحديث يكون من أولوياتها استحداث وحدات متخصصة لمكافحة جرائم تقنية المعلومات باعتبارها من الحلول العملية التي ستساعد سلطات التحقيق والعدالة الجنائية في التصدي لهذه الظاهرة، وتوفر فرصة لبناء كادر وظيفي متمكن وقادر على التعامل بكفاءة وفاعلية مع هذا النوع من الجرائم؛ الأمر الذي سيؤدي إلى سرعة الاستغناء عن خدمات الخبراء أو تقليل الاعتماد عليهم، وبالتالي ضمان العودة السريعة إلى رجال الضبط القضائي للإمساك بناصية التحقيق الجنائي.

رابعاً: التحقيق في جرائم تقنية المعلومات الموجهة ضد الأطفال

يعرَّف الطفل بأنه الصغير من كل مولود، ذكراً كان أو أنثى، ولم يصل إلى مرحلة الحلم.[72] وعرفت اتفاقية حقوق الطفل التي أقرتها الجمعية العامة للأمم المتحدة في المادة 1 من الجزء الأول الطفل بأنه كل إنسان لم يتجاوز سن الثامنة عشرة من العمر، ما لم تنص القوانين الوطنية على غير ذلك.[73]

لهذه الفئة العمرية خصائصها الجسمية والذهنية والنفسية التي تتشكل بموجبها انفعالاتها وسلوكها ورغباتها، وتعامل الآخرين معها، والمشكلات التي تصادفها، ومع ظهور التقنيات الحديثة، ممثلة في جهاز الحاسب الآلي وشبكة الإنترنت، شكلت هذه التقنيات جاذبية خاصة للأطفال في كافة المجتمعات، إلا أن أصحاب النزعات الجُرمية، دأبوا على الإيقاع بهذه الفئة البريئة من المجتمع، بوصفهم هدفاً مثالياً لأعمالهم الإجرامية، مستغلين ما

يتميزون به من براءة وسرعة ثقة بالآخرين، فضلاً عن الفضول وحب المغامرة التي تعتريهم، والرغبة الشديدة في جذب الانتباه لهم، وقد استغل أصحاب النفوس المريضة هذه المزايا عند الأطفال بهدف استدراجهم والإيقاع بهم ليكونوا ضحايا جرائمهم.

على سبيل المثال، فقد يبدأ المجرم في إقامة علاقة صداقة مع الطفل عن طريق شبكة الإنترنت من خلال التظاهر بمشاركته هواياته واهتماماته، وربما أدى هذا الأمر إلى تبادل الهدايا والصور، كما هو الحال بالنسبة للمجرمين التقليديين الذين يتصلون بصورة مباشرة مع الأطفال، إلا أن مجرمي الإنترنت عادة ما يكون لديهم استعداد كبير لقضاء أوقات طويلة في سبيل إقامة علاقة صداقة تقربهم من الطفل الضحية؛ الأمر الذي يزيد من فرص نجاحهم في تحقيق أغراضهم.[74]

ونظراً لأهمية هذا الموضوع في مجال التحقيق الجنائي لتعلقه بهذه الفئة التي تتطلب أساليب تحقيق تختلف عن الأساليب المتبعة لدى البالغين، فسوف نتناول في سياق هذا المبحث عوامل سقوط بعض الأطفال ضحايا أكثر من غيرهم، وبعض أنماط السلوك الإجرامي الذي يتبعه الجناة، والأساليب التي ينبغي اتباعها للتعامل مع الضحية في أثناء مرحلتي التحقيق والمحاكمة، ثم نعرض المعوقات التي تواجه جهاز التحقيق الجنائي، مسترشدين في ذلك بالتوجيهات التي تضمنتها النشرة الصادرة عن مكتب ضحايا الجريمة التابع لوزارة العدل الأمريكية.[75]

1. عوامل سقوط بعض الأطفال ضحايا الجريمة

رغم عدم استثناء أي أسرة من احتمال تعرض أبنائها للاستغلال أو الأذى عن طريق الإنترنت، فإن بعض الأطفال أكثر عرضة لهذا النوع من الجرائم من غيرهم، وهم:

1. الأطفال الأكبر سناً يتعرضون لمخاطر أكبر لكونهم يستخدمون أجهزة الحاسب الآلي وشبكة الإنترنت فترات أطول من غيرهم.
2. الأطفال الذين ينخرطون في مناقشة أمور شخصية على شبكة الإنترنت.
3. الأطفال الذين يشاركون في غرف الدردشة أو رسائل البريد الإلكتروني ويرسلون صوراً عبر شبكة الإنترنت.
4. المراهقون المترددون الذين يعانون بعض المشكلات النفسية نتيجة ضغوط ذويهم، ويسعون للتحرر منها.
5. الأطفال الذين يعانون حساسية مفرطة من الناحية العاطفية وينخرطون في محادثات تدغدغ مشاعرهم، وعادة ما تتسم هذه المحادثات في بادئ الأمر بالبراءة، إلا أنها سرعان ما تتحول إلى سلوك جنسي صريح.
6. الأطفال الذين تقل سلطة آبائهم عليهم أو تنعدم لأي سبب كان، فيصبحون بمنأى عن أي رقابة أو توجيه.

2. أنماط السلوك الإجرامي الموجه ضد الأطفال

يتبع مرتكبو جرائم الإنترنت أنماطاً مختلفة من السلوك للإيقاع بضحاياهم من الأطفال؛ ومن هذه الأنماط:

1. إغواء الضحايا عن طريق الاتصال بهم عبر الإنترنت بهدف استدراجهم وتوريطهم في ممارسات جنسية، بصورة مباشرة أو غير مباشرة.

2. استخدام الإنترنت لإنتاج وتصنيع وتوزيع الصور الإباحية للأطفال، وعادة ما يكون لهذا الأسلوب أثر أكبر في استدراج المراهقين والإيقاع بهم.

3. استخدام الإنترنت لغرض عرض الصور الإباحية على الأطفال وتشجيعهم على تبادل هذه الصور. وفي هذا السياق أوردت المنظمة الخيرية البريطانية (CH) في تقريرها السنوي ما يفيد بأن شبكة الإنترنت مسؤولة إلى حد كبير عن الارتفاع الهائل في نسبة الجرائم الإباحية الموجهة ضد الأطفال، حيث شهدت ارتفاعاً بنسبة 15 ضعفاً من عام 1988 حتى عام 2002؛ وذلك نتيجة للمواقع الإباحية والتقاط صور لمواضع جنسية مع الأطفال وتبادل تلك الصور معهم.[76]

4. استغلال الأطفال لأغراض تتعلق بالاتجار في المخدرات أو الاتجار في البشر "السفر بقصد الاشتراك في ممارسات جنسية" أو الحصول على مكاسب تجارية أو للإشباع الشخصي.

3. أساليب وطرق التعامل مع الأطفال الضحايا

في سبيل مواجهة هذا النوع من الجرائم الموجهة ضد الأطفال ينبغي على جهات التحقيق استخدام وسائل وطرق معينة لكسب ثقة الأطفال والوصول إلى المعلومات الصحيحة ومساعدة أسرهم على تجاوز محنتها، ومن هذه الأساليب ما يأتي:[77]

أ. بالنسبة للأطفال:

1. ينبغي على المحقق أن يحدد مستوى الطفل قبل سؤاله، بهدف اختيار اللغة والأفكار المناسبة لعمره ومستواه ومداركه.

2. على المحقق عدم الاستعانة بذوي الطفل إذا احتاج الأمر إلى مترجم لكون الأهل عادة يقحمون أنفسهم لتوجيه مسار التحقيق، وقد يحرفون رواية الطفل، ظناً منهم أن ذلك لمصلحته.

3. يجب على المحقق أن يتحلى بالصبر أثناء الاستجواب وألا يتعجل النتائج، فقد ينكر الضحية في البداية ومع مزيد من الدعم والتشجيع يصبح أكثر تجاوباً ويتبادل الحديث ويفشي بما كان يخفيه.

4. تجنب إجراء المقابلات المتعددة التي يتم خلالها سؤال ضحايا عدة في آن واحد؛ لأن ذلك سوف يؤدي إلى إرباك الأطفال وتخويفهم وتضارب أقوالهم.

5. ينبغي على المحقق ألا يظهر أي علامات للدهشة أو الصدمة؛ لأن ذلك سوف يزيد من إحراج الطفل ويشعره بالذنب فيقوم بتحوير الوقائع أو الامتناع عن ذكرها، مما يضر بمسار التحقيق والمحاكمة.

6. على المحقق أن يتحدث بصراحة مع الطفل، وأن يكون صادقاً في وعوده وتطميناته، وأن يزيل مخاوفه التي ربما تكون عالقة بذهنه بسبب تهديدات الجاني.

7. على المحقق مساعدة الطفل إذا كانت القضية من النوع الذي ستؤول إلى المحكمة، وأن يقوم بتهيئته لمثل هذه الأجواء؛ لأن الطفل الذي يتهيأ لدخول قاعة المحكمة يشارك بفاعلية أكبر في القضية.[78]

ب. بالنسبة للأسرة:

جرائم الإنترنت الواقعة على الأطفال تؤثر على الأسرة برمتها، وغالباً ما ينتاب أفرادها شعور بالذنب لعدم مقدرتهم على حماية أبنائهم، ويعتبرون ضحايا ثانويين؛ لذلك فهم بحاجة ماسة إلى الدعم والمساعدة، ومن أوجه ذلك:

1. تقديم العون المالي للأسرة، إذا تطلبت إجراءات التحقيق السفر إلى مناطق أو دول أخرى.

2. يجب تهيئة أفراد الأسرة للتغطية الإعلامية، ومساعدتها للتعامل مع وسائل الإعلام في حال تعرضهم لهذا الموقف.

3. الحرص على خصوصية الأسرة، والاستجابة قدر الإمكان لمطالبها فيما يتعلق بسرية التحقيق والمحاكمة.

4. مساعدة الأسرة على تفهم مشاعر الطفل الضحية حتى يستطيع بدوره تجاوز الموقف.

4. معوقات التحقيق الجنائي مع الأطفال

يتسم التحقيق مع الأطفال عموماً بالصعوبة والتعقيد، ويتطلب الصبر والروية في القضايا جميعها دون استثناء، ولكن هذه الصعوبة تزداد بالنسبة لجرائم تقنية المعلومات الواقعة على الأطفال؛ للاعتبارات الآتية:

1. هذا النوع من الجرائم يتطلب جهوداً مضاعفة، نظراً لطول الوقت الذي يفصل بين وقوع الفعل الإجرامي وبين إلقاء القبض على المجرم.

2. تعدد دوائر الاختصاص في ضوء خاصية الانتشار التي تمتاز بها جرائم تقنية المعلومات، مما يزيد من صعوبة مباشرة إجراءات التحقيق والمحاكمة.

3. عدم تعاون الأطفال "الضحايا" وذويهم مع جهات التحقيق، ويعدّ ذلك من أكبر المعوقات، ويأخذ الأشكال الآتية:

أ. عدم الرغبة في الحديث عن الجريمة أو إنكار حدوثها.

ب. ما ينتاب أفراد الأسرة من شعور بالخزي لتعرض أحد أبنائها للجريمة.

ج. الضغوط التي يتعرض لها الأطفال من أقرانهم.

د. الحرج الذي ينتاب الطفل عند التعرض للتفاصيل المتعلقة بالجوانب الجنسية.

هـ. التكاليف التي قد تتكبدها الأسرة إذا تتطلب الأمر انتقال الضحايا إلى مناطق أو دول أخرى ينعقد لها الاختصاص.

التحديات التي تواجه التحقيق الجنائي في جرائم تقنية المعلومات

إن أهم المعضلات الناجمة عن ظاهرة جرائم تقنية المعلومات هو ما تشكله هذه الظاهرة من تحد لسلطات التحقيق وأجهزة العدالة الجنائية، حيث أوضحنا في سياق عرضنا السابق أن طبيعة هذا النوع من الجرائم وخصائصها وسمات مرتكبيها قد وضعت الأجهزة المعنية بمكافحة الجريمة أمام تحديات جسام لم تكن مهيأة لها وليست قادرة على فهمها والتعامل معها.

والحقيقة أن هذه التحديات لا تتعلق باستعدادات الأجهزة التنفيذية وقدراتها وحسب، بل تتعداها إلى السلطات والأجهزة التشريعية والقضائية أيضاً، التي وضعت هي الأخرى أمام التحديات ذاتها؛ فليس بمقدور أجهزة التحقيق والعدالة الجنائية أن تعمل من دون مظلة تشريعية تضفي المشروعية على أعمالها وتحدد الأفعال المجَرَّمة من غيرها، وتضع القواعد الإجرائية والضوابط القانونية التي ينبغي لهذه الأجهزة اتباعها والتقيد بها.

وبالقدر نفسه من الأهمية، فإن الأمور لا تستقيم ما لم تكن الأجهزة القضائية على إلمام بالجوانب الفنية والعلمية لهذا النوع من الجرائم، بحيث تتوافر لديها القدرة على تقدير الأدلة ومعرفة طبيعة عمل الأجهزة المستخدمة ونظمها وفهم مصطلحاتها حتى تتمكن من إصدار الحكم فيها، وكذلك التعاطي القانوني مع مشكلة الاختصاص المرتبطة بطبيعة هذا النوع من الإجرام الذي يعمل في فضاءات مفتوحة لا تعترف بالحدود ولا تقيم وزناً لمبدأ السيادة.

أولاً: التحديات التشريعية في مجال قانون العقوبات وقانون الإجراءات الجزائية

1. في مجال قانون العقوبات

يتصدى قانون العقوبات للظواهر الإجرامية فيحدد الأفعال المجرمة ويضع العقوبات الرادعة لكل منها، وغايته إنزال العقاب بالمجرمين وحماية المجتمع من شرورهم وردع غيرهم عن الاقتداء بهم.[79]

لقد أفرزت جرائم تقنية المعلومات أنماطاً من الجرائم لم تخطر ببال المشرع وهو يضع القوانين ويحدد الجرائم وعقوباتها، وبعد انتشار هذا النوع من الجرائم تقاعس المشرع في الكثير من الدول، وبخاصة الدول العربية، عن تدارك النقص الذي يعتري التشريعات العقابية في هذا المجال، وترك أمر معالجتها للنصوص العقابية التقليدية والقواعد العامة، مما أوجد فراغاً تشريعياً اتضح من خلاله قصور هذه النصوص وعدم كفايتها لتغطية الأشكال المتنوعة لجرائم تقنية المعلومات.[80]

ولتجاوز هذه المشكلة لجأ بعض الفقهاء إلى الاجتهاد في تفسير النصوص القانونية العقابية التقليدية والتوسع فيها لجعلها تستوعب هذه الجرائم المستحدثة، إلا أن ذلك لم يفلح في تجاوز المشكلة نظراً لطبيعة جرائم تقنية المعلومات واختلاف صورها؛ الأمر الذي أدى ببعض الدول وخاصة الغربية منها إلى إصدار قوانين خاصة تتصدى لهذا النوع من الجرائم، ومثال ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا الصادر سنة 1999،[81] والقانون الفرنسي رقم 19 الصادر عام 1988 بشأن التحايل على نظم المعالجة الآلية للمعلومات وغيرها الكثير من الدول الغربية كالولايات المتحدة وكندا التي أصدرت قوانين مماثلة.[82]

وكان المشرع في دولة الإمارات العربية المتحدة قد تلمس هذه المشكلة وأدرك أهمية معالجتها، حيث صدر مؤخراً قانون جرائم تقنية المعلومات الاتحادي رقم 2/ 2006 الإماراتي المشار إليه سابقاً والذي حدد الأفعال غير المشروعة والعقوبات المقررة لها. وبهذا سدَّ النقص الذي كان يعانيه قانون العقوبات الاتحادي؛ الأمر الذي فتح المجال أمام سلطات التحقيق وأجهزة العدالة الجنائية والقضاء للسير قدماً في مواجهة هذا النوع من الجرائم، وبذلك لم تعد هناك أي مشكلة متعلقة بمشروعية الملاحقة الجزائية في ظل وجود النص التجريمي.

ب. في مجال قانون الإجراءات الجزائية

كما ذكرنا آنفاً، فإن قانون العقوبات يصف الأفعال غير المشروعة ويحدد عقوباتها بما يضفي المشروعية على ملاحقتها وضبط مرتكبيها ومعاقبتهم،

وهو يمثل الشق الأول من المعادلة التشريعية الجزائية، أما الشق الثاني فيتمثل في قانون الإجراءات الجزائية الذي يحدد القواعد الإجرائية والضمانات التي ينبغي أن تسير على هديها الجهات المعنية بإنفاذ القانون في مراحلها المختلفة، بدءاً بمرحلة الاستدلال وانتهاءً بالمحاكمة، فالقانونان إذن يكملان بعضهما بعضاً، فإذا كانت هناك حاجة إلى صدور قوانين عقابية خاصة بجرائم تقنية المعلومات، فإنه وبالقدر نفسه هناك ضرورة لصدور قوانين إجرائية تستجيب للمعطيات الجديدة التي أفرزتها هذه الجرائم، وتعالج المشكلات الناجمة عن تنفيذ الإجراءات التي تتطلبها عملية التحقيق؛ من معاينة وتفتيش وضبط وغيرها من إجراءات متعلقة بجرائم تقنية المعلومات التي لاتزال تثير جدلاً فقهياً حول قيمتها القانونية ومدى مشروعيتها.

وقد أشرنا سابقاً إلى الخلاف الفقهي الذي نشأ حول المكونات المعنوية ومدى خضوعها لإجراءات المعاينة والتفتيش والضبط في ظل القواعد الإجرائية التقليدية.[83] وعلى الرغم من أن النصوص القانونية في بعض الدول ومنها دولة الإمارات - كما أوضحنا - قد تضمنت ما يمكن تفسيره بقبول خضوع هذه المكونات لإجراءات التحقيق، فإن هذه المعالجة ليست كافية بل يجب تعزيزها بإصدار قوانين إجرائية تتصدى بشكل مباشر للجوانب الإجرائية لجرائم تقنية المعلومات كافة على غرار قانون العقوبات، وتعالج مشكلات الإثبات الجنائي ومدى مشروعية الأدلة، وتضع الضوابط للوصول إليها تفادياً لأي مشكلة قد يترتب عليها الإضرار بعملية التحقيق والطعن في مشروعية إجراءاتها.

ويلاحظ أن أهم الجوانب التي تتطلب المعالجة التشريعية في المجال الإجرائي لجرائم تقنية المعلومات ما يأتي:

1. صدور قانون ينظم إجراءات الضبط والتفتيش للكيانات المعنوية للحاسب الآلي ونظم تقنية المعلومات يأخذ في الاعتبار خصائص هذا النوع من الجرائم من حيث سرعة إخفاء الدليل وتدميره وعدم ترك آثار مادية، وذلك بمنح صلاحيات أوسع لسلطات التحقيق ورجال الضبط القضائي ليتمكنوا من تنفيذ هذه المهام بفاعلية، مع ضمان عدم انتهاك الحريات والحرمات وسيادة الدول.

2. إعادة النظر في مفهوم حالة التلبس القائم على معطيات مادية وحسية، حيث عرفت المادة 42 من قانون الإجراءات الجنائية الإماراتي الاتحادي رقم 35 لسنة 1992 حالة التلبس: «تعد الجريمة متلبساً بها إذا تبع المجني عليه مرتكبيها، أو تبعه العامة مع الصياح إثر وقوعها أو إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملاً آلات أو أسلحة أو متاعاً أو أشياء يستدل منها على أنه فاعل أو شريك فيها أو إذا وجدت به في هذا الوقت آثار أو علامات تفيد ذلك».

هذا النص لا يستقيم مع طبيعة جريمة تقنية المعلومات التي عادة لا يظهر منها أية إشارات أو معطيات مادية أو حسية، لذلك ينبغي تعديل هذه المادة بما يسمح بانطباقها على هذا النوع من الجرائم .

3. إضفاء صفة مأمور الضبط القضائي على خبراء الحاسب الآلي ونظم تقنية المعلومات الذين يتم الاستعانة بهم ليتمكنوا من القيام بالواجبات المنوطة بهم.

4. إيجاد الصيغة المناسبة لمعالجة مشكلة الاختصاص، حيث يمكن للجاني ارتكاب الجريمة من مسافات بعيدة بما يخرجه من دائرة الاختصاص المكاني للجهة القائمة على التحقيق.[84] وهذا الجانب غير منوط بالتشريعات الداخلية فحسب، وإنما يحتاج إلى تعاون دولي من خلال اتفاقيات ثنائية أو متعددة الأطراف أو تحت مظلة الأمم المتحدة.

ثانياً: التحديات في المجال الفني

أوضحنا فيما سبق أن إجراءات التحقيق في جرائم تقنية المعلومات لا تختلف، من حيث مراحلها الفنية التي نعرفها، عن الجرائم التقليدية.[85] إلا أن طبيعة هذه الجرائم وخصائصها وسمات مرتكبيها هي التي تختلف بصورة جذرية عن طبيعة وخصائص الجريمة التقليدية وسمات مرتكبيها، مما يشكل تحدياً كبيراً لسلطات التحقيق والعدالة الجنائية من حيث قدرة هذه الأجهزة على التعامل مع هذا النوع من الجرائم المستحدثة؛ وذلك للاعتبارات الآتية:

1. تتميز جرائم تقنية المعلومات بسرعة التخفي، بحيث يصعب على الشخص أو الجهة المعتدى عليها أن يلحظها، وربما لا يعلم بوقوعها إلا بعد حين أو عن طريق الصدفة، ومن هذه الجرائم: التلصص والتجسس عبر الإنترنت، وبث الفيروسات والقنابل الإلكترونية عبر البريد

الإلكتروني وعلى صفحات الإنترنت، وجرائم النصب والاحتيال. وعليه، فإن الطرق والأساليب التي تستخدم في ارتكاب جرائم تقنية المعلومات لم تعهدها الأجهزة المعنية بإنفاذ القانون، وماتزال وسائل هذه الأجهزة عاجزة عن الدخول في مواجهة مع مرتكبي هذا النوع من الجرائم بالكفاءة والفاعلية المطلوبتين.

2. في بعض الأحيان تفضل الشركات والمؤسسات المالية والأفراد التي تتعرض للاعتداء عدم الإبلاغ عن الجريمة؛ حفاظاً على سمعتها وعدم إثارة الشكوك حول موقعها المالي لضمان قيمة أسهمها في الأسواق المالية، ويبدو ذلك أكثر وضوحاً بالنسبة للجرائم التي تمس الأسرة والمخلة بالآداب العامة، فغالباً ما يتستر المجني عليهم على الجريمة حفاظاً على سمعتهم، وبخاصة في مجتمعاتنا المحافظة.[86]

3. إن جرائم تقنية المعلومات تتميز بسرعة تطور أساليبها في ضوء الابتكارات المتلاحقة في مجال تقنية المعلومات وبرامجها؛ مما ينعكس على أداء مرتكبيها الذين يطورون أساليبهم تبعاً لذلك، فيصبحون أكثر خطورة، الأمر الذي يتطلب من سلطات التحقيق والعدالة الجنائية مواكبة هذا التطوير والتمكن من أدواته، وهو ما يزيد من أعبائهم ويعظم من مسؤولياتهم.

4. إن هذه الجرائم ذات انتشار عالمي؛ فهي لا تعترف بالحدود الجغرافية بين الدول، وقد تمتد مساحة عملها لتغطي أنحاء العالم كافة لاستخدامها

شبكة الإنترنت، كما أن ضررها لا يقتصر على المجني عليه في مكان معين، بل يتعداه ليصيب مجموعات من المجني عليهم في أماكن أخرى، وهو ما نلحظه في جرائم تقنية المعلومات ذات الخطر على المعتقدات والرموز الدينية. وخير دليل على ذلك، واقعة الرسوم المسيئة لرسولنا محمد ﷺ، فقد أصاب ضررها المسلمين كافة في مغارب الأرض ومشارقها.

5. تتميز جرائم تقنية المعلومات بصعوبة إثباتها بالمقارنة مع الجرائم التقليدية، والحقيقة أن هذا الجانب يشكل أكبر التحديات التي تواجهها أجهزة إنفاذ القانون؛ وتتمثل هذه الصعوبة في النواحي الآتية:

أ. انعدام آثار الجريمة، حيث إن مرتكبي هذا النوع من الجرائم لا يخلفون آثاراً مادية ملموسة يمكن أن تشكل طرف خيط يقود إليهم، بفضل مهاراتهم في استخدام هذه التقنيات وبرامجها.[87]

ب. أن مرتكبي هذا النوع من الجرائم يحيطون أنفسهم بتدابير وقائية تزيد من صعوبة التعرف على أدلة الجريمة من خلال إجراءات الضبط والتفتيش، باستخدامهم شفرات أو كلمات سر أو برامج تشفير متطورة أو بروكسي أو تعليمات خفية تعمل على تدمير الأدلة بمجرد فتح الجهاز أو القيام بأي عملية من خلاله.[88] كما يستخدم هؤلاء الجناة وسائل وأدوات اتصال يصعب كشفها كالبريد الإلكتروني الذي يصعب من خلاله تسجيل المكالمات أو تحديدها، كما يحدث في الاتصالات السلكية واللاسلكية المعتادة.

ج. لا يستخدم هؤلاء الجناة في دخولهم شبكة الإنترنت أجهزتهم الخاصة في أغلب الأحيان، وإنما يلجؤون إلى مقاهي الإنترنت المنتشرة حالياً في معظم المدن والأحياء التي لا تتقيد بأي ضوابط أو أنظمة أمنية يمكن من خلالها التعرف على مستخدمي أجهزة الحاسب الآلي المتعاقبين في حالة اكتشاف أفعال غير مشروعة مصدرها هذه الأجهزة.[89]

د. أغلب البيانات والمعلومات التي يتم تداولها عبر الحاسب الآلي وشبكة الإنترنت هي عبارة عن رموز مخزنة على وسائط تخزين ممغنطة لا يمكن الوصول إليها إلا بواسطة الحاسب الآلي ومن قبل أشخاص قادرين على التعامل مع هذه الأجهزة ونظمها.[90]

هـ. قدرة الجناة في جرائم تقنية المعلومات على محو الدليل في زمن قياسي لا يتعدى ثواني معدودات، وذلك من خلال تعريض الوسائط الممغنطة لمجال مغناطيسي قوي قادر على محوها في لمح البصر.[91]

و. انتشار شبكات الـ (DSL) في المباني السكنية، وهو نظام يتم الدخول من خلاله إلى الخادم "مزود الخدمة" مباشرة دون وجود سجلات الكترونية (LOG FILS) لمستخدمي شبكة الإنترنت داخل تلك المباني، وكذلك انتشار شبكات اللاسلكي (WI FI) على نطاق واسع، بما يتيح لأي شخص استخدام حاسوبه المحمول في الدخول إلى الإنترنت من مكان تواجده دون قيود.

6. ما يتميز به مرتكبو جرائم تقنية الإنترنت من ذكاء ومعرفة علمية وفنية في مجال الحاسب الآلي ونظم تقنية المعلومات يشكل تحدياً كبيراً لرجال

السلطة العامة المعنيين بمكافحة هذه الجرائم، كونهم يتعاملون مع نوع جديد من الجناة الأذكياء لم يعهدوه من قبل.[92]

هذه التحديات المتعلقة بالجانب الفني لجرائم تقنية المعلومات تتطلب من مؤسسات الشرطة والنيابة العامة والقضاء تبني سياسات استراتيجية للتطوير والتنمية المستدامة لقواها البشرية، من خلال اعتماد برامج تدريب وتأهيل تغطي متطلبات عملية التحقيق كافة والمحاكمة لجرائم تقنية المعلومات.

ثالثاً: التحديات المتعلقة بالاختصاص والتعاون الدولي ومعوقاته

1. الاختصاص في مجال جرائم تقنية المعلومات

تعد جرائم تقنية المعلومات من أكثر الجرائم التي تثير مشكلات تتعلق بالاختصاص على المستويين المحلي والدولي؛ وذلك بسبب الطبيعة الخاصة لهذا النوع من الجرائم التي تمتاز بقدرتها على التحرك في مجال فضائي واسع لا توقفه حدود الدول وسيادتها الإقليمية، حيث يمكن لجريمة تقنية المعلومات أن تقع في مكان وتنتج آثارها في مكان أو أماكن أخرى داخل الدول أو خارجها.

هذا الواقع اصطدم بالتشريعات الجزائية المعمول بها اليوم في معظم دول العالم التي تأخذ بالطابع الإقليمي الذي يقيد سلطات التحقيق والعدالة الجنائية ويمنعها من مد صلاحياتها ومباشرة إجراءاتها الجنائية خارج نطاق حدود اختصاصها الإقليمي.[93]

ومن المعلوم أن هذه القوانين وضعت لتلبي متطلبات عملية التحقيق في الجرائم التقليدية التي يسهل معالجة مشكلات الاختصاص المتعلقة بها، سواء كان ذلك داخل النطاق الإقليمي للدولة من خلال الندب، أو خارج الحدود الإقليمية من خلال الاتفاقيات الثنائية أو الإقليمية أو الدولية المتعلقة بالتعاون الأمني والمساعدة القضائية بين الدول، والتي عادة ما تتطلب إجراءات إدارية تمر عبر مؤسسات بيروقراطية لا تتحملها مصلحة التحقيق في جرائم تقنية المعلومات نظراً لطبيعتها وخصائصها التي تتطلب سرعة التصرف لوقف مخاطرها وأضرارها وعدم تمكين الجناة من محو أو تدمير أدلة الإثبات، وبالتالي الإفلات من العقاب. هذا الأمر دفع بعض الدول إلى عقد اتفاقيات تعاون ثنائية أو عبر المنظمات الإقليمية والدولية التي ترعاها الأمم المتحدة؛ من أجل تسهيل القيام بإجراءات التحقيق فيما بينها كالضبط والتفتيش والقبض والاستجواب وتبادل المعلومات، غير أن الأمر يحتاج إلى مزيد من الإجراءات لمعالجة المشكلات المرتبطة بالاختصاص من خلال تعاون دولي أوثق وأشمل، يواكب تطور الوسائل التقنية في مجالي الاتصالات ونظم المعلومات، ويتجاوز المحاذير الإقليمية وحساسياتها.

2. التعاون الدولي في مجال جرائم تقنية المعلومات

بدأت الجهود الدولية الرامية إلى مواجهة التحديات التي تفرضها جرائم تقنية المعلومات منذ عام 1989 عندما اقترح المجلس الأوربي مجموعة من الإرشادات بشأن قوائم جرائم الحاسب الآلي والمشكلات

الناجمة عن الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، كما حض الدول الأعضاء على مراجعة قوانين الإجراءات الجزائية الوطنية لتتلاءم مع التطور الذي يشهده ارتفاع معدلات هذا النوع من الجرائم وانتشارها على نطاق واسع.[94]

ثم تبع ذلك مؤتمر الأمم المتحدة الثاني لمنع الجريمة ومعاملة المجرمين الذي انعقد في هافانا عام 1990، حيث أهاب في قراره الخاص بالجرائم ذات الصلة بالحاسب الآلي ونظم تقنية المعلومات بالدول الأعضاء تكثيف جهودها لضمان مكافحة فعالة لعمليات الاعتداء باستعمال الحاسب الآلي، وحضها على تطبيق إجراءات جنائية وتحديث القوانين واتخاذ تدابير على الصعيد الوطني؛ نذكر منها:

1. ضمان تطبيق القوانين الجزائية الراهنة المتعلقة بسلطات التحقيق وقبول الأدلة على نحو ملائم مع إدخال تغيرات مناسبة على هذه القوانين، إذا اقتضت الضرورة ذلك.

2. إصدار نصوص تشريعية إجرائية وموضوعية - كلما دعت الضرورة إلى ذلك - تختص بالتصدي لهذا الشكل الجديد والمعقد من النشاط الإجرامي، إذا لم تكن هناك نصوص تعالج ذلك.

كما حث المؤتمر الدول الأعضاء على مضاعفة الجهود على المستوى الدولي من أجل مكافحة الجرائم المتعلقة بالحاسب الآلي ونظم تقنية

المعلومات؛ من خلال انضمامها للمعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة في المسائل المرتبطة بهذا النوع من الجرائم. ونصح المؤتمر الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بهذه الموضوعات منطبقة انطباقاً كافياً على الأشكال الجديدة للإجرام المستحدث كجرائم تقنية المعلومات، وأن تتخذ خطوات محددة حسب الاقتضاء، من أجل تحقيق هذا الهدف، بالإضافة إلى خطوات أخرى أوصى المؤتمر بها، وأهمها تكفل قيام الدول الأعضاء بالعمل بفاعلية مع هذا النوع من الجرائم.[95]

لذلك يجب أن تحظى مهمة تعزيز التعاون الدولي في فتح آفاق جديدة في هذا المجال بالاهتمام اللازم، لضمان معالجة عملية وفعالة للمشكلات الإجرائية المرتبطة بجرائم تقنية المعلومات مع التركيز على إنجاز الخطوات الآتية:

1. وضع معايير دولية للجوانب الأمنية المتعلقة بالمعالجة الآلية للبيانات ونظم حمايتها.

2. وضع تدابير مناسبة لمعالجة المشكلات الناجمة عن الاختصاص التي تثيرها جرائم تقنية المعلومات العابرة للحدود وذات الطبيعة الدولية.[96] ويذكر في هذا المجال أن المجلس الأوربي في جلسته 13/ 95 بتاريخ 11 أيلول/ سبتمبر 1995 بشأن مشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، قد أشار إلى أن بيئة عمل إجراءات التحقيق في مجال جرائم تقنية المعلومات قد تقتضي التدخل السريع لمد الإجراءات إلى أنظمة حاسبات موجودة خارج الدول القائمة على التحقيق، وحتى لا

يمثل ذلك اعتداءً على سيادة هذه الدول أو على القانون الدولي، ينبغي وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، لذلك ثمة حاجة ملحة إلى إبرام اتفاقيات تنظم كيفية اتخاذ مثل هذه الإجراءات. كما أوصى المجلس بضرورة اتخاذ إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة واتخاذ إجراءات التفتيش والضبط، وكذلك السماح لهذه الجهات بإجراء تسجيلات للتعاملات ذات الصلة بالسلوك الإجرامي المرتكب وتحديد مصادره، وهو ما يوجب تطوير اتفاقيات التعاون الدولي القائمة.[97]

3. تعزيز التعاون الدولي في مجال تسليم الأشخاص وتجسيد إجراءات المساعدة القانونية والقضائية، حتى خلال إبرام اتفاقيات على المستوى الثنائي الإقليمي والدولي.

4. توحيد المفاهيم المتعلقة بجرائم تقنية المعلومات وتنسيق الجهود لوضع تصور موحد لها وتحديد صورها ومن ثم تعميمها على الدول الأعضاء بالأمم المتحدة، حتى لا يحدث اختلاف حول تجريم أفعال في دولة دون أخرى؛ الأمر الذي يعوق سبل التعاون الدولي في هذا المجال.

3. معوقات التعاون الدولي في مجال جرائم تقنية المعلومات

يشكل التعاون الدولي في مجال جرائم تقنية المعلومات حجر الأساس في بناء نظام قادر على خوض مواجهة فعالة لهذا النوع من الجرائم، إلا أن هناك

عقبات تعترض سبيل إنجاح هذا التعاون وتحقيق غاياته المرجوة ومن أبرز هذه العقبات ما يأتي:

1. صعوبة الاتفاق على مفهوم محدد لجريمة تقنية المعلومات؛ بسبب اختلاف المفاهيم والقيم الاجتماعية والأخلاقية بين المجتمعات، وهذا يؤدي إلى تجريم الأفعال في بعض الدول دون أخرى، الأمر الذي يعوق التعاون في مجالات المساعدة القضائية وتسليم المجرمين.

2. اختلاف أساليب التعامل مع هذا النوع من الجرائم، بسبب تباين النظم القانونية بين الدول.

3. صعوبة معالجة المشكلات القانونية والفنية المرتبطة بإجراءات التفتيش والضبط والملاحقة خارج النطاق الإقليمي.

4. عدم كفاية الاتفاقيات المتعلقة بتسليم الأشخاص والمساعدة القضائية، مما يعرقل إجراءات التحقيق وتأخير البت بها.

الدراسة المسحية لعينة من المحققين منتسبي القيادة العامة للشرطة ـ أبوظبي

أولاً: أسباب اقتصار الدراسة المسحية الإحصائية على إمارة أبوظبي

يقتصر النطاق الجغرافي لهذه الدراسة على إمارة أبوظبي دون أن تشمل الإمارات الأخرى التي تتكون منها دولة الإمارات العربية المتحدة، وهذا المنحى له أسبابه الوجيهة المستندة إلى طبيعة النظام الإداري والدستوري

لدولة الإمارات العربية المتحدة، التي تتكون من اتحاد فيدرالي تجتمع فيه الكثير من خصائص الدولة الوحدوية.[98] وتبعاً لذلك، فإن الأساس القانوني لنظام الشرطة في دولة الإمارات العربية المتحدة قد حدده الدستور المؤقت الصادر عام 1971 الذي نص في مادته رقم 138 من الباب التاسع « يكون للاتحاد قوات مسلحة برية وبحرية وجوية موحدة التدريب والقيادة، ويكون تعيين القائد لهذه القوات ورئيس الأركان العامة وإعفاؤهما من منصبيهما بمرسوم اتحادي، كما يجوز أن يكون للاتحاد قوات أمن اتحادية».

يستشف من هذا النص إجازته قيام قوات أمن اتحادية إلى جانب قوات الأمن المحلية أو عوضاً عنها، التي كانت قائمة بالفعل قبل الاتحاد، وإن كانت هذه الإجازة صريحة إلا أنها جاءت في حكم الاستثناء، والقاعدة أن يكون لكل إمارة عضو في الاتحاد قوات أمن محلية خاصة بها.

وفي إطار سعي الحكومات المحلية الأعضاء في الاتحاد في كل من إمارات؛ رأس الخيمة، وأم القيوين، وعجمان، والفجيرة لتكريس مسيرة الاتحاد، وحرصها على عدم حدوث تضارب بين الأجهزة الاتحادية ووصيفتها المحلية، قررت هذه الحكومات في عام 1974 ضم أجهزتها الأمنية المحلية إلى جسم وزارة الداخلية الاتحادية، ثم تبعتها بعد عام شرطة إمارة الشارقة، ولم يبق خارج جسم الوزارة الاتحادية سوى جهازي شرطة إمارة دبي، وإمارة أبوظبي اللتين ظلتا تابعتين للسلطات الإدارية والتنظيمية والمالية للحكومتين المحليتين في كل من أبوظبي ودبي.[99]

في ظل هذا الوضع لم يكن من المجدي أن يمتد نطاق هـذه الدراسـة إلى المحققين في أجهزة التحقيق الجنائي على مستوى المؤسسات الشرطية في دولة الإمارات العربية المتحدة، باعتبار أن هذه المؤسـسات تتكـون مـن وحـدات إدارية وتنظيمية وهيكليـة مـستقلة. وبالتـالي، فلكـل وحـدة منهـا معطياتهـا ومـشكلاتها ومنـاهج عملهـا، لـذلك ارتأينـا أن تقتـصر العينـة الإحـصائية المستهدفة على المحققين في إمـارة أبوظبي لضمان السيطرة على محـددات هـذه الدراسة والاستفادة من مخرجاتها بالنسبة للمـديريات الـثلاث التـي تتكـون منها القيـادة العامـة لـشرطـة أبـوظبي، وهـي: مديريـة شرطـة العاصـمة، ومديرية شرطة العين، ومديرية شرطة طريف.

ثانياً: العينة الإحصائية

لاختبار فرضية الدراسة المتمثلة في أن أجهزة التحقيق الجنـائي في إمـارة أبوظبي غير مؤهلة من الناحية الفنية على التعامل مع جرائم تقنية المعلومـات بالكفاءة والفاعلية المطلوبة، قام الباحث بإجراء دراسة مسحية على عينة مـن المحققين في مراكز الـشرطة المختـصة بفـتح البلاغـات وتلقـي الـشكاوى في المديريات الثلاث التي تتكون منها القيادة العامة للشرطة في إمارة أبوظبي.

يتبع المديريات الثلاث 24 مركزاً مختصاً بأعمال جمع الاستدلالات، وقد تم حصر تلك المراكز واختيار عينة عشوائية مكونة من عشرة مراكز مـن بـين المراكز الأكبر حجماً والأكثر تغطية، وقد وزعت الاستبانة على عشرة محققـين من كل مركز بمجموع مئة محقق في المراكز العشرة موزعين على النحو التالي:

- مديرية شرطة العاصمة: أربعة مراكز، عشرة محققين من كل مركز، مجموع 40 محققاً.

- مديرية شرطة العين: أربعة مراكز، عشرة محققين من كل مركز، مجموع 40 محققاً.

- مديرية شرطة طريف: مركزان، عشرة محققين من كل مركز، مجموع 20 محققاً.

ثالثاً: أداة الدراسة

يبين الملحق (الاستبانة) التي استخدمت في هذه الدراسة والمكونة من عشرة أسئلة، حيث تم اختيار فقراتها بعناية فائقة، وبعد دراسة الجوانب المختلفة لمشكلة الدراسة يمكن تصنيف الفقرات التي تتكون منها الاستبانة إلى المجموعات الآتية:

المجموعة الأولى: بيانات خاصة بالثقافة العامة للمحقق في مجال الحاسب الآلي وجرائم تقنية المعلومات؛ انظر الفقرات (1 و 2 و 3 و 4 و5).

المجموعة الثانية: بيانات خاصة بالتعرف على القدرات التقنية لدى المحققين للتعامل مع هذا النوع من الجرائم؛ انظر الفقرات (6 و 7و 8 و 9).

المجموعة الثالثة: بيانات خاصة بالتعرف على قدرات المحققين في المجال التشريعي؛ انظر الفقرة (10).

وقد سبق توزيع الاستبانة بشكلها النهائي اختبار مدى صدقها وثباتها، وذلك من خلال توزيعها على عينتين استطلاعيتين وتحكيمها من خلال ثلاثة خبراء في مجال القياس والتقويم، وقد تبين أن أداة الدراسة صادقة، كما أن نتائجها تتصف بالثبات والدقة. والمقصود بصدق أداة القياس أنها تقيس حقيقة الغرض الذي صممت من أجله ويعرف هذا بصدق المحتوى CONTENT VALIDITY، كما يقاس صدق الأداء من خلال عرضها على محكمين لتقييمها، والمقصود بثبات الأداء INSTRUMENT RELIABILITY أن نتائج الاستبانة لا تختلف عند تطبيقها على عينات متعددة، أما المقصود بالعينة الاستطلاعية PILOT SAMPLE فهي عينة صغيرة يتم تطبيق الأداة عليها قبل تعميمها؛ بغية اكتشاف أي خلل في فقراتها لمعالجته.

رابعاً: تحليل البيانات واختبار الفرضيات

سبق أن ذكرنا أن الفرضية التي يهدف هذا البحث إلى اختبارها تنص على أنه لا يوجد لدى المحققين في إمارة أبوظبي التأهيل الكافي والمهارات التقنية في التعامل مع جرائم تقنية المعلومات من الناحيتين الفنية والعلمية.

وللتحقق من هذه الفرضية تم توزيع استبانة على مئة من المحققين موزعين على عشرة مراكز رئيسية لاستطلاع آرائهم في هذا المجال، وفيما يلي عرض لنتائج تحليل الاستبانة:

1. ثقافة المحققين في مجال تقنية المعلومات

تم توجيه الأسئلة الخمسة التالية لتحديد ثقافة المحققين في مجال تقنية المعلومات.

- السؤال الأول: هل تشكل القرصنة بواسطة الحاسب الآلي مشكلة أمنية؟
- السؤال الثاني: هل التحقت بدورات متخصصة في مجال الحاسب الآلي؟
- السؤال الثالث: ما مدى الدور الذي يلعبه الحاسب الآلي في حياتنا اليومية؟
- السؤال الرابع: هل من الضروري إدخال جهاز الحاسب الآلي في مجال عمل أجهزة التحقيق الجنائي؟
- السؤال الخامس: معدلات جرائم الحاسب الآلي والإنترنت؛ تزداد أم تتناقص؟

وأبرز ما يمكن استخلاصه من تحليل الإجابات عن تلك الأسئلة ما يلي:

السؤال الأول: هل تشكل القرصنة بواسطة الحاسب الآلي مشكلة أمنية؟

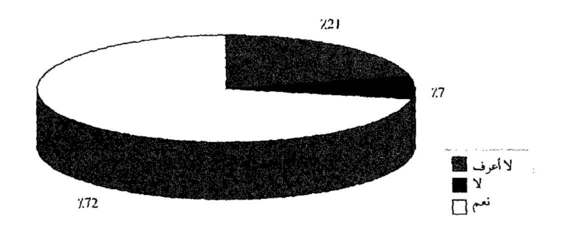
الإجابة: نعم (72) لا (7) لا أعرف (21)

يتبين من تحليل الإجابات عن هذا السؤال بأن 72٪ من عينة المحققين الذين شملتهم هذه الدراسة مقتنع بأن القرصنة بواسطة الحاسب الآلي تشكل جريمة أمنية، وأنها بهذا المفهوم تدخل في مجال اختصاصهم وتؤثر على

مستوى أدائهم لأعمالهم. ولا تزيد نسبة الذين لا يعتقدون بذلك على 7٪ فقط، بينما أجاب 21٪ بأنهم لا يعرفون الإجابة عن هذا السؤال، وهي نسبة عالية في الواقع، خاصة وأننا نتكلم عن عينة من المحققين وليس من عامة الناس. ويشير (الشكل 1) إلى تدني المستوى المعرفي لهذه الفئة لعدم إدراكهم مخاطر جريمة القرصنة أو عدم فهمهم لمعناها.

الشكل (1)

هل تشكل القرصنة بواسطة الحاسب الآلي مشكلة أمنية؟

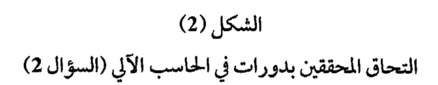


السؤال الثاني: هل التحقت بدورات متخصصة في مجال الحاسب الآلي؟

الإجابة: نعم (84)   لا (16)

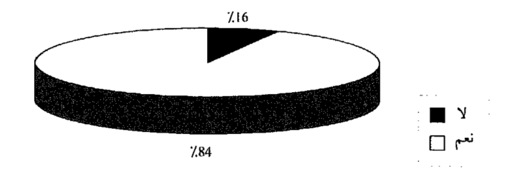
تظهر هذه الإجابة بأن الغالبية العظمى من العاملين في مجال التحقيق الجنائي (84٪) قد تلقوا دورات تدريبية، وقد تبين للباحث لدى مراجعته فرع التدريب والتطوير أن هذه الدورات تقتصر على برامج الطباعة وليس

من بينها أي دورة متعلقة بالجريمة المعلوماتية، وهو مؤشر على خلل في سياسة التدريب المتبعة يتمثل في عدم تبني برامج تدريب للعاملين في مجال التحقيق الجنائي تؤهلهم للتعامل مع هذا النوع من الجرائم.



الشكل (2)

التحاق المحققين بدورات في الحاسب الآلي (السؤال 2)



السؤال الثالث: ما مدى الدور الذي يلعبه الحاسب الآلي في حياتنا اليومية؟

الإجابة: حيوي (91)   بسيط (8)   غير حيوي (1)

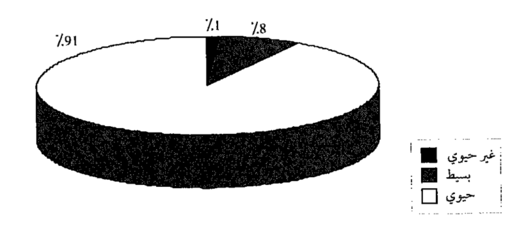
على الرغم من أن الدورات التي تلقاها المحققون بدائية لا تتعدى استخدام جهاز الحاسب الآلي في مجال الطباعة، فإنها كونت لديهم قناعات أولية بأهمية الحاسب الآلي في مختلف مناشط الحياة اليومية، يبدو ذلك واضحاً من خلال إجاباتهم عن هذا السؤال.

فقد أجاب 91٪ من المحققين بأن دور الحاسب الآلي في حياتهم اليومية دور حيوي، بينما أجاب 1٪ من المحققين بأنه دور غير حيوي، وأجاب 8٪

من المحققين بأن الحاسب الآلي له دور بسيط في حياتهم اليومية. وهذا يبين أن الغالبية العظمى من المحققين تدرك أهمية هذه التقنية ودورها الحيوي في أوجه الحياة المختلفة، حتى وإن كانت تلك الغالبية غير مدربة تدريباً كافياً على استخدام تلك التقنية، (انظر الشكل 3).

الشكل (3)

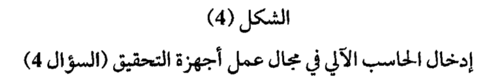
دور الحاسب الآلي في حياتنا اليومية (السؤال 3)



السؤال الرابع: هل من الضروري إدخال جهاز الحاسب الآلي في مجال عمل أجهزة التحقيق؟

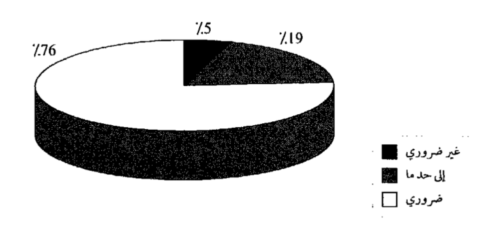
الإجابة: ضروري (76)　　إلى حد ما (19)　　غير ضروري (5)

تظهر هذه الإجابة أن 76٪ من المشاركين قد أكدوا ضرورة إدخال هذه التقنية في مجال عملهم، وهو مؤشر على أن معظم المشاركين يدركون الحاجة إلى هذه التقنية في مجال عمل التحقيق الجنائي، وهي نسبة مرتفعة تزيد على الثلثين، (انظر الشكل رقم 4).



الشكل (4)

إدخال الحاسب الآلي في مجال عمل أجهزة التحقيق (السؤال 4)



السؤال الخامس: معدلات جرائم الحاسب الآلي والإنترنت في تزايد أم نقصان؟

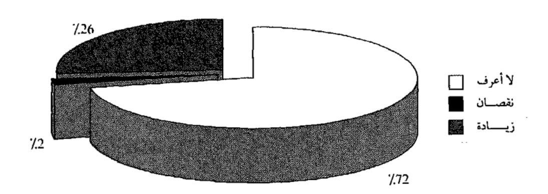
الإجابة: زيادة (26) نقصان (2) لا أعرف (72)

لا تقوم الإجابة في الفئتين الأولى والثانية على أي أساس معرفي قائم على التجربة أو البيانات الإحصائية، لعدم توافرها أصلاً، وإنما اعتمدت على الحدس والتخمين، وتشير إجابة الفئة الثالثة إلى أن 72٪، وهي نسبة تزيد على ثلثي المشاركين، لا يستطيعون تحديد موقفهم من معدلات الجريمة المعلوماتية واتجاهاتها لنفس السبب الذي أشرنا إليه والمتمثل في أن العاملين في جهاز التحقيق لم يتعاملوا بالمطلق مع هذا النوع من الجرائم، وهي نتيجة منطقية تنسجم مع الواقع.

الشكل (5)

تغير معدلات جرائم الإنترنت

معدلات جرائم الحاسب الآلي والإنترنت؛ في تزايد أم نقصان؟



2. قدرات المحققين في التعامل مع جرائم تقنية المعلومات من الناحيتين الفنية والقانونية

ويشمل هذا الجانب معظم فقرات الاستبانة ويتكون من الأسئلة الآتية:

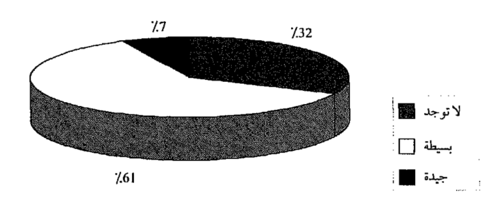
- السؤال (6): هل لديك معلومات عن أي من جرائم الحاسب الآلي والإنترنت؟
- السؤال (7): هل تعاملت مع جريمة أو أكثر من جرائم تقنية المعلومات؟
- السؤال (8): هل يوجد فرق بين المتسللين وقراصنة الحاسب الآلي والإنترنت؟
- السؤال (9): هل تتطلب جرائم تقنية المعلومات تغييراً في أساليب التحقيق؟

السؤال السادس: هل لديك معلومات عن جرائم الحاسب الآلي والإنترنت؟

الإجابة: جيدة (7)   بسيطة (61)   لا توجد (32)

الشكل (6)

معلومات المحققين عن جرائم تقنية المعلومات



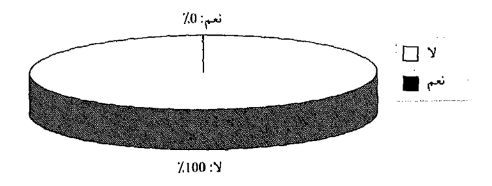
يتضح أن أغلبية المشاركين (61٪) أفادوا بأن لديهم معلومات بسيطة عن الجريمة المعلوماتية، وأن نسبة الذين لا توجد لديهم معلومات مطلقاً تأتي في المرتبة الثانية بنسبة 32٪، ولما كانت المعلومات التي لا يتردد صاحبها في وصفها بالبسيطة لا تكفي للتعامل الناجح في مجال التحقيق في جرائم تقنية المعلومات الذي يتميز بالتعقيد والصعوبة، فإنه من الممكن استنتاج أن نسبة 94٪ على الأقل من المحققين في إمارة أبوظبي يجهلون أساليب التحقيق في هذا النوع من الجرائم.

السؤال السابع: هل تعاملت مع جريمة أو أكثر من جرائم تقنية المعلومات؟

الإجابة: نعم (0)   لا (100)

تظهر هذه الإجابة أن أفراد العينة لم يتعاملوا على الإطلاق مع أي نوع من الجرائم المعلوماتية، وهو ما تأكد للباحث من خلال مراجعته للبيانات الإحصائية الجرمية الصادرة عن دائرة السجلات بشرطة أبوظبي والتي لم يظهر فيها أي جريمة من هذا النوع، وذلك لا يعني عدم حدوث جرائم من هذا النوع وإنما يشير إلى عدم تعامل سلطات التحقيق وأجهزة الشرطة معها حتى الآن، وبالتالي فإن هذا النوع من الإجابات لا يحتاج إلى مزيد من الإيضاحات.

الشكل (7)



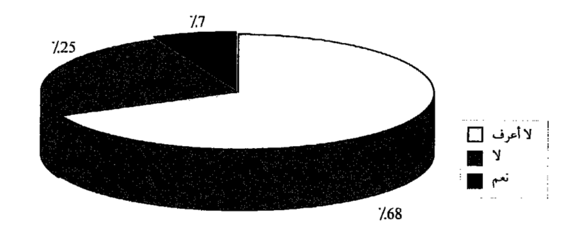
السؤال الثامن: هل يوجد فرق بين المتسللين وبين قراصنة الحاسب الآلي والإنترنت؟

الإجابة: نعم (7)   لا (25)   لا أعرف (68)

تشير الإجابة إلى أن ما يزيد على ثلثي أفراد العينة تقريباً (68٪) لا يعرفون الفرق بين المتسللين والقراصنة فضلاً عن أن نسبة (25٪) لم يميزوا بين المتسللين والقراصنة، وهو مؤشر على جهل أفراد العينة حين يكون السؤال متعلقاً بالجوانب الأكثر دقة وتخصصاً، وهذا يشير، مع نتائج السؤال السابق، إلى أن ثقافة العاملين في جهاز التحقيق قائمة على معلومات عامة، وأن الغالبية العظمى منهم لا يملكون المعلومات الدقيقة، وهو ناجم عن عدم التأهيل والتدريب وانعدام الخبرة، (انظر الشكل 8).

الشكل (8)

هل يوجد فرق بين المتسللين وبين قراصنة الكمبيوتر والإنترنت؟



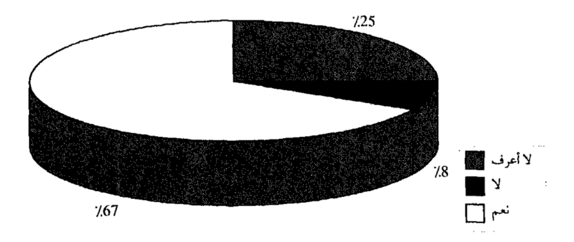
السؤال التاسع: هل تتطلب جرائم تقنية المعلومات تغيراً في أساليب التحقيق؟

الإجابة: نعم (67) لا (8) لا أعرف (25)

تشير هذه الإجابة إلى أن نسبة الثلثين من المستطلعين لديها شعور بأهمية تغيير أساليب التحقيق لتتكيف مع المعطيات الجديدة التي فرضتها جرائم تقنية المعلومات، وأن نسبة 25٪ بالإضافة إلى 8٪ وهم يمثلون نسبة 33٪ من العينات لا يدركون الحاجة إلى هذا التغيير، وهو مؤشر على تدني ثقافة هذه الفئة في مجال جرائم تقنية المعلومات، وهو ما يتوافق مع النتائج التي أسفرت عنها الإجابات عن الأسئلة السابقة المتعلقة بالجانب الفني.

الشكل (9)

هل تتطلب جرائم الكمبيوتر والإنترنت تغيراً في أساليب التحقيق؟



يتبين من تحليل نتائج الاستبانة الخاصة بالأسئلة المتعلقة بالجانب الفني، أن الغالبية المطلقة من المحققين الحاليين يؤمنون بأن جرائم تقنية المعلومات تشكل نوعاً جديداً من الجرائم غير مفهومة بالنسبة لهم، وأن التحقيق فيها يتطلب الدراية والمعرفة التقنية في مجال الحاسب الآلي ونظم تقنية المعلومات.

أما الفقرة المتعلقة بالجانب التشريعي فقد أجاب المستطلعون عن السؤال التالي:

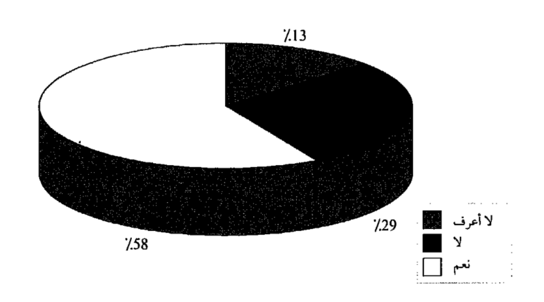
السؤال العاشر: هل التشريعات الجزائية كافية لمواجهة جرائم تقنية المعلومات؟

الإجابة: نعم (58)   لا (29)   لا أعرف (13)

يتضح أن نسبة 58٪ من العينة يعتبرون التشريعات الحالية كافية، وهي نتيجة طبيعية في ضوء صدور قانون جرائم تقنية المعلومات الاتحادي 2/ 2006 الذي غطى النقص التشريعي بالنسبة للشق الموضوعي، أما نسبة 29٪ الذين أجابوا بعدم كفايتها فذلك ناجم إما عن عدم علمهم بصدور القانون نظراً لحداثته، أو اعتباره غير كاف لعدم صدور قانون يعالج الشق الإجرائي، وأجاب 13٪ بعدم معرفتهم بموضوع السؤال، وهو مؤشر على نقص الثقافة القانونية بالنسبة لهذه الفئة.

(الشكل 10)

هل التشريعات الجزائية الحالية كافية لمواجهة هذا النوع من الجرائم؟



الخاتمة

عالجت هذه الدراسة موضوع التحقيق في جرائم تقنية المعلومات الذي تباشره سلطات التحقيق وأجهزة العدالة الجنائية، وقد قدم الباحث عرضاً مركزاً للجوانب النظرية والعملية المتصلة بهذا النوع من الجرائم.

تناول الباحث مفاهيم جرائم تقنية المعلومات والتصنيفات المتعلقة بها من خلال موقفين؛ الأول يعكس المفاهيم الغربية العلمانية. والثاني يعبر عن المفاهيم العربية والإسلامية، وعرض نموذجين لكل منهما، ثم قام الباحث بتصنيف هذه الجرائم في ضوء القانون الخاص بجرائم تقنية المعلومات الإماراتي الذي صدر مؤخراً، وتعد هذه الدراسة هي الأولى التي تأخذ هذا المنحى من التصنيف، فقد استوقف الباحث خلوُّ التشريعات الجزائية الغربية من النصوص التي تجرم الانتهاكات الماسة بالمعتقدات الدينية، وندرتها بالنسبة للانتهاكات المتعلقة بالآداب العامة والقيم الأسرية، ورد ذلك إلى المفاهيم السائدة واختلافها بين الجانبين، كما أن التصنيف الذي عرضه الباحث، وفق قانون جرائم تقنية المعلومات الإماراتي، غير مسبوق أيضاً، نظراً لحداثة هذا القانون.

كما تناول الباحث بالشرح إجراءات التحقيق الجنائي بمرحلتي جمع الاستدلالات والتحقيق، مقترحاً استحداث وحدات متخصصة تلحق بمراكز التحقيق الرئيسية، على أن يتم تدريب وتأهيل كوادرها ليكونوا قادرين على التعامل بكفاءة وفاعلية مع هذا النوع من الجرائم المستحدثة،

ووضع من خلال هذا المقترح آلية للتعاون بين الخبير والمحقق في إطار عمل هذه الوحدات، كما تناول موضوع التحقيق في هذا النوع من الجرائم الموجهة ضد الأطفال، نظراً لما يتطلبه التعامل مع الأطفال من إجراءات خاصة تختلف عن إجراءات التعامل مع البالغين.

وتناول الباحث التحديات التي تواجه عملية التحقيق الجنائي من جوانبها التشريعية والفنية والمسائل المتعلقة بالاختصاص والتعاون الدولي، وأشار إلى أن صدور قانون جرائم تقنية المعلومات قد عالج الجانب الموضوعي من المشكلة التشريعية، إلا أنه مايزال هناك قصور بالنسبة للجانب الإجرائي الذي ينبغي تغطيته، لضمان مواجهة قانونية ناجحة وفعالة مع مرتكبي هذا النوع من الجرائم.

ولإثبات فرضية الدراسة القائمة على أن المحققين لا تتوافر لديهم المعارف المهنية اللازمة للتعامل مع هذه الجرائم، قام الباحث بإجراء دراسة مسحية أجاب عنها مئة من المحققين في المديريات التابعة للقيادة العامة للشرطة في إمارة أبوظبي التي تضمنها الفصل الأخير من هذه الدراسة، حيث تبين من خلال تحليل نتائج الاستبانة صدقية الفرضية، وأن المحققين الجنائيين ليسوا مؤهلين من الناحيتين النظرية والعملية للتعامل مع هذا النوع من الجرائم؛ الأمر الذي يقتضي إعادة النظر في الأساليب المتبعة لمواكبة التطور في مجال الجريمة المعلوماتية.

وقد انتهى الباحث إلى عدد من التوصيات والنتائج التي يعتقد أنها ستسهم - حال تطبيقها - في حل الكثير من المشكلات القائمة، وستؤدي إلى

رفع كفاءة وفاعلية أجهزة التحقيق والبحث الجنائي، ومدها بالوسائل التقنية والتشريعية، وكذلك وضع المعالجات المناسبة لمشكلة الاختصاص وإجراءات الملاحقة والضبط والتفتيش، انطلاقاً من إدراك الباحث لحقيقة أن التخلف عن خوض غمار هذه المواجهة سيؤدي إلى تفاقم المشكلات الأمنية ويلحق ضرراً لا تحمد عقباه في مجمل مناحي الحياة الاقتصادية والاجتماعية والأخلاقية والعقائدية، فليس هناك من خيار أمام الأجهزة المعنية بالدفاع الاجتماعي ضد الجريمة سوى السير قدماً في طريق المواجهة القائمة على المعرفة العلمية الرصينة والكفاءة التقنية العالية في الجوانب المتصلة بهذه الجرائم كافة، في سبيل مكافحتها والوقاية منها.

نتائج الدراسة

من خلال ما تقدم وفي ضوء الدراسة المسحية، توصل الباحث إلى النتائج الآتية:

1. المحققون الجنائيون في إمارة أبوظبي لا يتمتعون بالمهارات الفنية والخبرات العملية للتعامل مع جرائم تقنية المعلومات.
2. انعدام الدورات المتخصصة في مجال الجريمة المعلوماتية، وهذا ناجم عن قصور في سياسات إدارة التدريب والتطوير.
3. أجهزة التحقيق في مديريات كل من العاصمة ـ العين ـ طريف تعاني نقصاً شديداً في المعلومات المتعلقة بأنواع الجرائم المعلوماتية.
4. ضآلة المعرفة بالمصطلحات المتعلقة بالجرائم المعلوماتية.

5. وجود شعور عام بضرورة تغيير أساليب التحقيق الحالية.

6. هناك قصور في معرفة المنتسبين العاملين بمجال التحقيق والبحث الجنائي في القيادة العامة للشرطة/ أبوظبي لقانون جرائم تقنية المعلومات الإماراتي، الذي صدر مؤخراً.

7. اختلاف المفاهيم المتعلقة بجرائم تقنية المعلومات بين اتجاهين؛ أحدهما يمثل النظرة الغربية، والآخر يمثل النظرة العربية والإسلامية.

التوصيات

في ضوء ما تقدم يتضح أن جرائم تقنية المعلومات قد أحدثت تغييراً كبيراً في المفاهيم ذات الصلة بالتحقيق الجنائي، كما أن هذا النوع من الجرائم أفرز واقعاً جديداً ضاعف من حجم التحديات التي تواجهها الأجهزة المعنية بالدفاع الاجتماعي ضد الجريمة التي تقف اليوم أمام مفترق طرق لا خيار فيه سوى السير في اتجاه إعادة صياغة أساليبها ومناهجها وحتى هياكلها التنظيمية، وبدون ذلك لا يمكن لهذه الأجهزة أن تعمل بكفاءة وفاعلية في مواجهة هذه الجرائم العصرية المعقدة، وفي هذا السياق يقترح الباحث التوصيات الآتية:

1. استحداث وحدات متخصصة في مجال جرائم تقنية المعلومات تلحق بأقسام ومراكز التحقيق في مديريات الشرطة، يتم اختيار عناصرها من العاملين في مجال التحقيق ممن لديهم المقدرة والاستعداد على التكيف

مع تقنيات الحاسب الآلي بحيث توكل إليهم، دون غيرهم، مهمة التعامل مع هذا النوع من الجرائم.

2. إرسال العاملين في هذه الوحدات إلى دورات خارجية متخصصة في إجراءات التحقيق والبحث الجنائي في جرائم تقنية المعلومات، في الدول التي تتمتع بمعارف وخبرات عالية في هذا المجال.

3. إيجاد الصيغة المثلى للتعاون بين أجهزة التحقيق الجنائي وبين الخبراء في مجال الحاسب الآلي ونظم المعلومات، بغية إسناد جهاز التحقيق بالجوانب الفنية الأكثر تعقيداً، والتي تحتاج إلى مهارات متقدمة وخبرات متخصصة.

4. تدريب العناصر السرية "المصادر" على أساليب البحث والتحري وجمع المعلومات في مجال جرائم تقنية المعلومات، ونشرهم في الأماكن التي يعتقد أن تكون بؤراً يتجمع فيها الشباب والمراهقون، كمقاهي الإنترنت المنتشرة حالياً في الكثير من المدن.

5. تعميم نظام بيانات المستخدم، الذي طبقته مديرية شرطة العين وألزمت مقاهي الإنترنت بالتقيد به وأن يعمم على كافة مديريات الشرطة، الأمر الذي سيعزز القدرة على التحكم والسيطرة، ويحد من استخدام هذه الأماكن لمقاصد جرمية.

6. تشكيل لجنة من الأكاديميين والمهنيين المتخصصين وسلطات التحقيق الجنائي للنظر في قانون الإجراءات الجزائية الحالي وتعديله بما يتفق

والمعطيات الجديدة التي فرضتها جرائم تقنية المعلومات على الصعيد الإجرائي وتحدياتها؛ ليتوافق مع شقه الآخر قانون العقوبات الاتحادي 2/ 2006 بشأن جرائم تقنية المعلومات الذي صدر مؤخراً.

7. إطلاق حملة توعية من خلال المحاضرات والندوات عبر وسائل الإعلام لتوضيح مخاطر جرائم تقنية المعلومات لفئة المراهقين والشباب وطلاب المدارس والجامعات، وشرح مضامين قانون جرائم تقنية المعلومات الاتحادي وتبيان الأفعال المجرمة وتصنيفاتها وأنواعها في ضوء نصوص هذا القانون.

8. الدخول في اتفاقيات دولية ثنائية وإقليمية للتعاون في مجال تطبيق إجراءات التحقيق الجنائي المتعلقة بجرائم تقنية المعلومات ومعالجة مشكلة الاختصاص التي تفرضها الطبيعة الخاصة لهذه الجرائم.

9. التعاون في إطار جامعة الدول العربية ومجلس التعاون لدول الخليج العربية في المجالات التشريعية وتوحيد المفاهيم المتعلقة بجرائم تقنية المعلومات.

الملحق

استبيان

السؤال الأول: هل تشكل القرصنة بواسطة الكمبيوتر مشكلة أمنية؟

الإجــابـة

نعم	لا	لا أعرف

السؤال الثاني: هل التحقت بدورات حاسب آلي أو إنترنت؟

الإجــابة

نعم	لا

السؤال الثالث: ما مدى الدور الذي يلعبه جهاز الكمبيوتر في حياتنا اليومية؟

الإجــابـة

حيوي	بسيط	غير مهم

السؤال الرابع: هل من ضرورة لإدخال جهاز الكمبيوتر في مجال عمل أجهزة التحقيق الجنائي؟

الإجــابـة

ضرورة ملحة	إلى حد ما	غير ضروري

السؤال الخامس: هل معدلات جرائم الحاسب الآلي والإنترنت تزداد أو تتناقص؟

الإجـــابـة

زيادة	نقصان	لا أعرف

السؤال السادس: هل لديك معلومات عن أي من جرائم الحاسب الآلي والإنترنت؟

الإجـــابـة

وافية	بسيطة	لا يوجد

السؤال السابع: هل تعاملت مع جريمة أو أكثر من جرائم الحاسب الآلي والإنترنت؟

الإجـــابـة

نعم	لا

السؤال الثامن: هل يوجد فرق بين المتسللين وبين قراصنة الكمبيوتر والإنترنت؟

الإجـــابـة

نعم	لا	لا أعرف

السؤال التاسع: هل تتطلب جرائم الكمبيوتر والإنترنت تغييراً في أساليب التحقيق الحالية؟

الإجـــابـة

نعم	لا	لا أعرف

السؤال العاشر: هل التشريعات الجزائية الحالية كافية لمواجهة هذا النوع من الجرائم؟

الإجـــابـة

نعم	لا	لا أعرف

الهوامش

1. أبو بكر الرازي، **مختار الصحاح**، (بيروت: دار الكتاب العربي، 1982).

2. عبدالنور عبدالله الشحي، **التحقيق في مواجهة جرائم الحاسب الآلي والإنترنت**، دراسة مقدمة لجائزة مجلس التعاون الخليجي، 2002، العين، دولة الإمارات العربية المتحدة، ص9.

3. علي محمود علي حمودة، "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، بحث مقدم إلى المؤتمر العلمي الأول حول **الجوانب القانونية والأمنية للعمليات الإلكترونية**، دبي، دولة الإمارات العربية المتحدة، 26-28 نيسان/ إبريل 2003، مجلد 1، محور القانون الجنائي، ص200.

4. أحمد عبدالكريم سلامة، "الإنترنت والقانون الخاص: فراق أم تلاق؟" بحث مقدم إلى مؤتمر **القانون والكمبيوتر والإنترنت**، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة من 1-3 مايو 2000، المجلد الثالث، ص 25.

5. يونس عرب، **قانون الكمبيوتر**، (بيروت: منشورات اتحاد المصارف العربية، الطبعة الأولى، 2000)، ص3.

6. المرجع السابق.

7. إسماعيل عبد النبي شاهين، "أمن المعلومات في الإنترنت بين الشريعة والقانون"، بحث مقدم إلى مؤتمر **القانون والكمبيوتر والإنترنت**، كلية الشريعة، جامعة الإمارات، العين، 2000، ص974.

8. عبدالنور عبدالله الشحي، مرجع سابق، ص 11.

9. وليد عاكوم، "التحقيق في جرائم الحاسوب"، بحث مقدم إلى المؤتمر العلمي الأول حول **الجوانب القانونية للعمليات الإلكترونية**، دبي، دولة الإمارات العربية المتحدة، مجلد 1، محور القانون الجنائي، من 26-28 إبريل 2003، ص522.

10. اللوديون هم جماعة إنجليزية ظهرت في أواخر القرن التاسع عشر، يعتقدون أن الآلات سوف تؤدي إلى تناقص الطلب على الأيدي العاملة، جريدة الرياض، 9/ 11/ 2001، شبكة الإنترنت، الموقع www. A badrani. net.

11. عامر نزار وفايز أبوعلي، فيروسات الكمبيوتر، (عمان: دار حنين للطباعة والنشر، 1994)، ص17.

12. هشام رستم، "الجرائم المعلوماتية، أصول التحقيق الجنائي والفني، اقتراح إنشاء آلية عربية موحدة للتدريب التخصصي"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، العين، جامعة الإمارات العربية، كلية الشريعة والقانون، من 1-3 مايو 2000، المجلد الثاني، ط 2004، ص 451.

13. عبدالنور عبدالله الشحي، مصدر سابق، ص 12.

14. محمد عبدالرحيم العلماء، "جرائم الإنترنت والاحتساب عليها"، بحث مقدم إلى مؤتمر القانون والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000، المجلد الثالث، ص 879.

15. أثارت هذه الحادثة احتجاجات عاصفة عمت العالمين العربي والإسلامي، وأدت إلى مقاطعة المنتجات الدنماركية على نطاق شبه كامل، المصدر: وكالات الأنباء، موقع هيئة الإذاعة البريطانية BBC Arabic.com، تاريخ النشر 30/ 1/ 2006.

16. عرفت المذكرة التي أقرتها الأمانة العامة لمجلس وزراء الداخلية العرب رقم 622 الصادرة بتاريخ 9/ 5/ 2005 الجرائم المستحدثة بأنها «أفعال غير مشروعة وغير مألوفة تستجيب لبعض المتغيرات الاجتماعية أو السياسية أو الاقتصادية أو التكنولوجية المعاصرة وتشيع أخطاراً بالأفراد، وقد تلحق أضراراً بهم أو بالمجتمع أو البيئة المحيطة بها، الأمر الذي يستوجب تدخل المجتمع بآليات قانونية أو أمنية لمواجهتها، والحد منها». المصدر: أرشيف القيادة العامة لشرطة أبوظبي.

17. هشام رستم، مرجع سابق، ص411.

18. المرجع السابق، ص 405.

19. هلالي عبد الإله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، (القاهرة: دار النهضة العربية، طبعة عام 2000)، ص 13، انظر:

Laslie D .Ball , computer crime ," in *formation technology revolution* " edited and introduced press, Cambridge , 1985, 544 by Tom forester the mit.

20. هشام رستم، مرجع سابق، ص 2.

21. علي محمود حمودة، "الأدلة المتحصلة في الوسائل الإلكترونية"، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 26- 28 نيسان/ إبريل 2003، مجلد (1)، مرجع سابق، ص239.

22. علي عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، (الإسكندرية: دار الجامعة الجديدة للنشر، 1997)، ص2.

23. انظر:

David Thompson, "Current Trends in Computer Control Crime", *Computer Quarterly*, vol , 9, No.1, 1991. 20.

24. انظر:

Artur Solarz, "Computer – Related Embezzlement", *Computers and Security*, vol. 6, No.1, 1987, 52.

25. نقلاً عن هشام رستم، الجرائم المعلوماتية، مرجع سابق، ص 407.

26. القانون الاتحادي الإماراتي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية لدولة الإمارات العربية المتحدة، شباط/ فبراير 2006.

27. المصدر: يونس عرب، ورقة عمل بعنوان "الجرائم السيبرونية" المقدمة إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبوظبي 10- 12/ 2/ 2002، انظر الموقع:

www.arab law .org\down load\cyber crimes_work paper.doc

28. عبدالنور عبدالله الشحي، مرجع سابق، ص 14.

29. ممدوح عبدالحميد، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت)، (الشارقة: دار الفتح للطباعة والنشر، الطبعة الأولى، 2000)، ص 212.

30. ممدوح عبدالحميد، المرجع السابق ص 213.

31. يونس عرب، "جرائم الكمبيوتر والإنترنت"، نشرة اتحاد المصارف العربية، دورية شهرية، بيروت، لبنان، العدد 25، 2003.

32. ورد هذا التصنيف في بحث للدكتور محمد عبدالرحيم العلماء أستاذ الفقه والأصول المساعد بقسم الدراسات الإسلامية ومساعد العميد لشؤون البحث العلمي بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة بعنوان "جرائم الإنترنت والاحتساب عليها" المقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته جامعة الإمارات بالتعاون مع كل من مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة خلال الفترة 1-3 أيار/ مايو 2000، المجلد الثالث، الطبعة الثالثة، 2004، ص 779 وما بعدها.

33. تعرض أحد المقيمين في مدينة العين بإمارة أبوظبي إلى واقعة نصب واحتيال عن طريق الإنترنت من قبل عصابة أبلغوه، من خلال بريده الإلكتروني، بأنه ربح مبلغ 250 ألفاً، وأنه لن يتم تحرير المبلغ إلا إذا سدد قيمة الضرائب والرسوم واستخراج شهادات الحالة الأمنية التي كانوا يطلبونها على مراحل، والتي بلغ مجموعها 44 ألفاً، فقام بإرسالها إليهم عن طريق الحوالات السريعة (ويسترن يونيون)، وعندما طلبوا منه إرسال مبلغ إضافي مقابل إفادة لإثبات أن المال الذي سيحول إليه ليس من الاتجار بالمخدرات اكتشف أنه وقع في مكيدة، فقام بإبلاغ الشرطة بالواقعة. المصدر: أرشيف مديرية شرطة العين/ قسم شرطة المقام/ بلاغ رقم 257/ 2007.

34. في إحدى الوقائع التي حدثت في منطقة الوثبة بإمارة أبوظبي قام أحد الأشخاص بتصوير فتاة وهو معها في وضع مخل بالآداب العامة، ونشر الصور عبر هاتفه النقال بواسطة البلوتوث، وبعد ضبطه من قبل الشرطة اعترف بتصوير الفتاة بقصد التفاخر بين الشباب، وقام بنسخ الفيلم على حاسبه الآلي، زاعماً أن أحد القراصنة استطاع

نسخ الصور وإرسالها إلى أصدقائه، فانتشرت كالنار في الهشيم، ولم يستطع تدارك الأمر، وقد حكم على الجاني بالجلد والحبس سنة. المصدر: مجلة الشرطة، مجلة شهرية للدراسات والثقافة الشرطية والمجتمع، تصدر عن وزارة الداخلية بدولة الإمارات العربية والمتحدة، العدد 426، حزيران/ يونيو 2006، ص27.

35. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، (القاهرة: دار الجليل للطباعة، الطبعة 13، 1989)، ص 249.

36. محمد أمين البشري، "التحقيق في جرائم الحاسب الآلي والإنترنت"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت بجامعة الإمارات العربية المتحدة 1- 3/ 5/ 2000، المجلد الثالث، الطبعة الثالثة، ص 1048.

37. المرجع السابق، ص 1050.

38. قانون الإجراءات الجزائية الإماراتي الاتحادي، رقم 87 لسنة 1992.

39. تنص المادة 35 من قانون الإجراءات الجزائية الإماراتي أنه يجب على مأموري الضبط القضائي أن يقبلوا البلاغات والشكاوى التي ترد إليهم في شأن الجرائم، ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على الإيضاحات وإجراءات المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلمون بها بأي كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة.

40. محمد غيث، معاينة مسرح الجريمة، رسالة دكتوراه، (أكاديمية العلوم الشرطية، كلية الدراسات العليا، القاهرة، 1982)، ص 13.

41. علي محمود علي حمودة، الجوانب القانونية الأمنية للعمليات الإلكترونية، مجلد رقم (1)، محور القانون الجنائي، مرجع سابق، ص 216.

42. عبدالله حسين علي محمود، "إجراءات جمع الأدلة في مجال سرقة المعلومات"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، 26-28 نيسان/ إبريل 2003، ص 9.

43. هشام رستم، مرجع سابق، ص 86.

44. المرجع السابق، ص 87.

45. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، (القاهرة: دار الجليل للطباعة، الطبعة 13، 1989)، مرجع سابق، ص 264.

46. محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الجزء الثاني، التفتيش والضبط، (القاهرة: دار النهضة العربية، 1978)، ص114.

47. هلالي عبد الإله أحمد، مفتش نظم الحاسب الآلي وضمانات المعلومات، (القاهرة: دار النهضة العربية، طبعة 1997)، ص84.

48. علي محمود حمودة، مرجع سابق، ص 224 وما بعدها.

49. عبدالله حسين علي محمود، "إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات"، مرجع سابق، ص 14.

50. حسن سعيد الغافري، "التحقيق والأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص20، منشور بموقع المنشاوي للدراسات والبحوث www.Minshawi.com، نقلاً عن:

Irini Vassilaki: Computer crimes and other crimes against information technology in Greece. Rev. Inter De .Pen 1990, 37.

51. علي محمود حمودة، مرجع سابق، ص225، نقلاً عن:

Donald k. Piragoff: Computer crimes and other crimes against information trechnology in Canada Rev.intern De. Dr Pen 1993, 241.

52. المادة 53 من قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة رقم 35 لسنة 1992.

53. المادتان 96 و 40 من قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة رقم 35 لسنة 1992.

54. المادة 55 من القانون رقم 35 أعلاه.

55. محمد أبو العلا عقيدة، "التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية"، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 26 - 28 نيسان/ إبريل 2003، مجلد 1، محور القانون الجنائي، ص 33.

56. رؤوف عبيد، مرجع سابق، ص 330.

57. عبدالله حسين علي محمود، مرجع سابق، ص 33.

58. المرجع السابق، ص 24.

59. محمد أبو العلا عقيدة، مرجع سابق، ص 37.

60. علي محمود علي حمودة، مرجع سابق، ص 293.

61. حازم نعيم الصمادي، الشمولية في العمليات المصرفية الإلكترونية، (عمان: دار وائل للنشر، طبعة 2003)، ص 29 وما بعدها.

62. عبدالله حسين محمود، مرجع سابق، ص 36.

63. هشام رستم، الجوانب الإجرائية للبرامج المعلوماتية، دراسة مقارنة، (أسيوط: مكتبة الآلات الحديثة، 1994)، ص 18 و 19.

64. هشام رستم، المرجع السابق، ص 100.

65. محمد أمين البشري، "التحقيق في جرائم الحاسب الآلي"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، من 1-3/ 5/ 2000، ط 2004، مرجع سابق، ص 1072.

66. محمد أمين البشري، المرجع السابق، ص 1073.

67. عبدالرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، (القاهرة: دار النهضة العربية، طبعة 2000)، ص 447 و448.

68. د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في الجرائم الإلكترونية، ص 27، نقلاً عن أحكام محكمة النقض، الدائرة الجنائية، نقض 4/ 1/ 1983، س 34، رقم 5، ص52.

69. المادة 96 من قانون الإجراءات الجزائية الاتحادي، دولة الإمارات العربية المتحدة، رقم 87 لسنة 1992.

70. هشام رستم، مرجع سابق، ص 140 و 141.

71. المرجع السابق، ص487.

72. ابن منظور، لسان العرب ، (بيروت: مطبعة دار لسان العرب، ص599).

73. اتفاقية حقوق الطفل الصادرة التي أقرتها الجمعية العامة للأمم المتحدة رقم 44 / 25 في 20 نوفمبر 1989، انظر في ذلك: www.Unicef.Org\arabic\crc\files .crc_arabic.pdf

74. عاكف يوسف صوفان، "مشكلات النمو وأمن الطفل"، بحث منشور بمجلة الفكر الشرطي الصادرة عن مركز البحوث بشرطة، الشارقة، مجلد 12، عدد 2، 2003، ص66.

75. انظر: الدورية الشهرية الصادرة عن مركز دعم القرار التابع للقيادة العامة لشرطة دبي، دولة الإمارات العربية المتحدة، عدد 128، آب/ أغسطس 2002.

76. موقع الإذاعة البريطانية BBC Arabic.com ، تاريخ النشر 9 آذار/ مارس 2004.

77. بشير البلبيسي، دور الشرطة في حماية الأطفال من العنف وإساءة المعاملة، صادرة عن مركز البحوث والدراسات الشرطية، شرطة أبوظبي، دراسة 28/ 2004، ص 85.

78. المرجع السابق، ص 99.

79. محمد محيي الدين عوض، "مشكلات السياسة الجنائية المعاصرة"، بحث مقدم لمؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص 42.

80. علي محمود علي حمودة، مرجع سابق، ص 233.

81. المرجع السابق، ص 269.

82. هدى حامد قشقوش، "الإتلاف غير العمدي لبرامج وبيانات الحاسب الآلي"، بحث مقدم لمؤتمر القانون والإنترنت، 1–3 أيار/ مايو 2000، الطبعة الثالثة، 2004، المجلد الثالث، ص 903.

83. أحمد يوسف وهدان، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، (الشارقة: الفكر الشرطي، دورية ربع سنوية، تصدر عن الإدارة العامة لشرطة الشارقة، مركز بحوث الشرطة، مجلد 13 عدد 1، نيسان/ إبريل 2004.

84. زكي زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي، (القاهرة: دار النهضة العربية، سنة 1993)، ص 476.

85. محمد أمين البشري، التحقيق الجنائي المتكامل، الرياض، (الرياض: أكاديمية نايف للعلوم الأمنية، 1997)، ص 57.

86. في إحدى الوقائع الشهيرة تعرض بنك MARCHANT BANK CITY في بريطانيا لنقل ثمانية ملايين جنيه من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ، لكن البنك وبدلاً من تقديم شكوى قام بدفع مبلغ مليون جنيه للجاني، شريطة عدم إعلام الآخرين عن الجريمة، انظر: يونس عرب، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية، عمان، 1994، ص 72.

87. جميل عبدالباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، (القاهرة: دار النهضة العربية، 1992)، ص22.

88. يذكر أن أحد الأشخاص طلب مبلغاً من المال من إحدى الشركات مدعياً أنه وضع قنبلة منطقية في نظام حواسيبها، ولما استعانت الشركة بخبير للتحقق من صحة الادعاء وإبطال مفعول القنبلة ، نجح بالفعل في إبطال مفعول القنبلة وإزالتها من جزء من البرنامج الموضوعة فيه، وعندما تولت الشرطة التحقيق تبين إزالة كل الأدلة على وجود القنبلة. انظر في ذلك: هشام رستم، مرجع سابق، ص 339.

89. طبقت مديرية شرطة العين في أيار/ مايو 2006 نظاماً ألزمت فيه مقاهي الإنترنت في المدينة بتسجيل البيانات الشخصية لمستخدمي أجهزة الحاسوب في المقهى على بطاقات توضح تاريخ ويوم ووقت الاستخدام ومدته، المصدر: أرشيف مديرية شرطة العين.

90. جميل عبدالباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (القاهرة: دار النهضة، طبعة 2001)، ص113.

91. ما شهدته دولة الإمارات العربية المتحدة من وقائع، ومنها قيام أحد موظفي القطاع الخاص عام 1996 بتهديد مسؤولي إحدى الشركات بمحو كافة بيانات الشركة المخزنة بأنظمة الحاسب الآلي إن لم تستجب لمطالبه الوظيفية، وما لبث أن قام بتنفيذ تهديده ثم أقدم على الانتحار؛ الأمر الذي ألحق بالشركة أضراراً كبيرة وصعوبات جمة لاسترجاع هذه البيانات.

المصدر: خالد البستاني ورقة عمل بعنوان "أمن المعلومات وتحليل المخاطر" مقدمة لندوة فيروسات الحاسب الآلي، التي عقدها معهد التنمية الإدارية بالمجمع الثقافي بأبوظبي في 23 أيلول/ سبتمبر 1996، وذكرها هشام رستم، مرجع سابق، ص430.

92. غنام محمد غنام، "عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر"، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية، العين، 1-3/ 5/ 2000، المجلد الثاني، الطبعة الثالثة، 2004، ص، 628.

93. محمد أمين البشري، مرجع سابق، ص 1078.

94. أحمد يوسف وهدان، مرجع سابق، ص 112.

95. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت،(القاهرة: دار النهضة العربية، 2000)، ص 8.

96. أحمد يوسف وهدان، مرجع سابق، ص 114.

97. انظر: هشام رستم، تقرير مقدم لمؤتمر الأمم المتحدة التاسع لمكافحة الجريمة ومعاملة المجرمين، القاهرة، 1995، المنشور بمجلة الدراسات القانونية الصادرة عن كلية الحقوق بجامعة أسيوط، 1996، ص 10.

98. محمد عبيد الحساوي، "نظام الشرطة في دولة الإمارات العربية المتحدة"، مجلة الفكر الشرطي، الشارقة، دولة الإمارات العربية المتحدة، المجلد الخامس، العدد الثاني، 1996، ص 273.

99. المرجع السابق، 282.

نبذة عن المؤلف

راشد بشير إبراهيم: حاصل على درجة الماجستير في القانون الجنائي من جامعة العلوم التطبيقية والاجتماعية بصنعاء عام 2006، ودرجة الليسانس في الحقوق من جامعة عين شمس بالقاهرة عام 1983، والدبلوم العالي في الدراسات القانونية الدولية من معهد القانون الدولي بالتعاون مع جامعة الإسكندرية عام 1999.

زاول مهنة المحاماة في فلسطين عام 1986، وعمل مستشاراً للجنة التأسيسية لجامعة العين للعلوم والتكنولوجيا بدولة الإمارات العربية المتحدة، ووضع نظامها القانوني (2002-2004). وشارك محاضراً في العديد من الدورات التدريبية وتأهيل الضباط والمستجدين الجنائيين. ويعمل حالياً بمهنة باحث بالقيادة العامة لشرطة أبوظبي/ مديرية شرطة العين- فرع التخطيط والدراسات.

أصدر العديد من الأبحاث في المجالات القانونية المتنوعة (القانون الجنائي، قانون العقوبات، القانون الدولي، نظام البيئة). وكتب العديد من المقالات في الصحف المحلية بدولة الإمارات العربية المتحدة.

صدر من سلسلة «دراسات استراتيجية»

العدد	المؤلف	العنوان
.1	جيمس لي ري	الحروب في العالم: الاتجاهات العالمية ومستقبل الشرق الأوسط
.2	ديفيد جارنم	مستلزمات الردع: مفاتيح التحكم بسلوك الخصم
.3	هيثم الكيلاني	التسوية السلمية للصراع العربي - الإسرائيلي وتأثيرها في الأمن العربي
.4	هوشانج أمير أحمدي	النفط في مطلع القرن الحادي والعشرين: تفاعل بين قوى السوق والسياسة
.5	حيدر بدوي صادق	مستقبل الدبلوماسية في ظل الواقع الإعلامي والاتصالي الحديث: البعد العربي
.6	هيثم الكيلاني	تركيا والعرب: دراسة في العلاقات العربية التركية
.7	سمير الزبن ونبيل السهلي	القدس معضلة السلام
.8	أحمد حسين الرفاعي	أثر السوق الأوروبية الموحدة على القطاع المصرفي الأوربي والمصارف العربية
.9	سامي الخزندار	المسلمون والأوربيون: نحو أسلوب أفضل للتعايش
.10	عوني عبدالرحمن السبعاوي	إسرائيل ومشاريع المياه التركية: مستقبل الجوار المائي العربي
.11	نبيل السهلي	تطور الاقتصاد الإسرائيلي 1948 - 1996
.12	عبدالفتاح الرشدان	العرب والجماعة الأوربية في عالم متغير

27. صالح محمود القاسم — الديمقراطية والحرب في الشرق الأوسط خلال الفترة 1945 - 1989
28. فايز سارة — الجيش الإسرائيلي: الخلفية، الواقع، المستقبل
29. عدنان محمد هياجنة — دبلوماسية الدول العظمى في ظل النظام الدولي تجاه العالم العربي
30. جلال الدين عزالدين علي — الصراع الداخلي في إسرائيل (دراسة استكشافية أولية)
31. سعد ناجي جواد وعبدالسلام إبراهيم بغدادي — الأمن القومي العربي ودول الجوار الأفريقي
32. هيل عجمي جميل — الاستثمار الأجنبي المباشر الخاص في الدول النامية: الحجم والاتجاه والمستقبل
33. كمال محمد الأسطل — نحو صياغة نظرية لأمن دول مجلس التعاون لدول الخليج العربية
34. عصام فاهم العامري — خصائص ترسانة إسرائيل النووية وبناء «الشرق الأوسط الجديد»
35. علي محمود العائدي — الإعلام العربي أمام التحديات المعاصرة
36. مصطفى حسين المتوكل — محددات الطاقة الضريبية في الدول النامية مع دراسة للطاقة الضريبية في اليمن
37. أحمد محمد الرشيدي — التسوية السلمية لمنازعات الحدود والمنازعات الإقليمية في العلاقات الدولية المعاصرة
38. إبراهيم خالد عبدالكريم — الاستراتيجية الإسرائيلية إزاء شبه الجزيرة العربية
39. جمال عبدالكريم الشلبي — التحول الديمقراطي وحرية الصحافة في الأردن
40. أحمد سليم البرصان — إسرائيل والولايات المتحدة الأمريكية وحرب حزيران/ يونيو 1967

.41	حسن بكر أحمد	العلاقات العربية - التركية بين الحاضر والمستقبل
.42	عبدالقادر محمد فهمي	دور الصين في البنية الهيكلية للنظام الدولي
.43	عوني عبدالرحمن السبعاوي وعبدالجبار عبد مصطفى النعيمي	العلاقات الخليجية - التركية: معطيات الواقع، وآفاق المستقبل
.44	إبراهيم سليمان مهنا	التحضر وهيمنة المدن الرئيسية في الدول العربية: أبعاد وآثار على التنمية المستدامة
.45	محمد صالح العجيلي	دولة الإمارات العربية المتحدة: دراسة في الجغرافيا السياسية
.46	موسى السيد علي	القضية الكردية في العراق: من الاستنزاف إلى تهديد الجغرافيا السياسية
.47	سمير أحمد الزبن	النظام العربي: ماضيه، حاضره، مستقبله
.48	الصوفي ولد الشيباني ولد إبراهيم	التنمية وهجرة الأدمغة في العالم العربي
.49	باسيل يوسف باسيل	سيادة الدول في ضوء الحماية الدولية لحقوق الإنسان
.50	عبدالرزاق فريد المالكي	ظاهرة الطلاق في دولة الإمارات العربية المتحدة: أسبابه واتجاهاته - مخاطره وحلوله (دراسة ميدانية)
.51	شذا جمال خطيب	الأزمة المالية والنقدية في دول جنوب شرقي آسيا
.52	عبداللطيف محمود محمد	موقع التعليم لدى طرفي الصراع العربي - الإسرائيلي في مرحلة المواجهة المسلحة والحشد الأيديولوجي
.53	جورج شكري كتن	العلاقات الروسية - العربية في القرن العشرين وآفاقها
.54	علي أحمد فياض	مكانة حق العودة في الفكر السياسي الفلسطيني
.55	مصطفى عبدالواحد الولي	أمن إسرائيل: الجوهر والأبعاد
.56	خيرالدين نصر عبدالرحمن	آسيا مسرح حرب عالمية محتملة
.57	عبدالله يوسف سهر محمد	مؤسسات الاستشراق والسياسة الغربية تجاه العرب والمسلمين

58.	علي أسعد وطفة	واقع التنشئة الاجتماعية واتجاهاتها: دراسة ميدانية عن محافظة القنيطرة السورية
59.	هيثم أحمد مزاحم	حزب العمل الإسرائيلي 1968 - 1999
60.	منقذ محمد داغر	علاقة الفساد الإداري بالخصائص الفردية والتنظيمية لموظفي الحكومة ومنظماتها (حالة دراسية من دولة عربية)
61.	رضا عبدالجبار الشمري	البيئة الطبيعية في دول مجلس التعاون لدول الخليج العربية والاستراتيجية المطلوبة
62.	خليل إسماعيل الحديثي	الوظيفية والنهج الوظيفي في نطاق جامعة الدول العربية
63.	علي سيد فؤاد النقر	السياسة الخارجية اليابانية دراسة تطبيقية على شرق آسيا
64.	خالد محمد الجمعة	آلية تسوية المنازعات في منظمة التجارة العالمية
65.	عبدالخالق عبدالله	المبادرات والاستجابات في السياسة الخارجية لدولة الإمارات العربية المتحدة
66.	إسماعيل عبدالفتاح عبدالكافي	التعليم والهوية في العالم المعاصر (مع التطبيق على مصر)
67.	الطاهرة السيد محمد حمية	سياسات التكيف الاقتصادي المدعمة بالصندوق أو من خارجه: عرض للدراسات
68.	عصام سليمان الموسى	تطوير الثقافة الجماهيرية العربية
69.	علي أسعد وطفة	التربية إزاء تحديات التعصب والعنف في العالم العربي
70.	أسامة عبدالمجيد العاني	المنظور الإسلامي للتنمية البشرية

71.	حمد علي السليطي	التعليم والتنمية البشرية في دول مجلس التعاون لدول الخليج العربية: دراسة تحليلية
72.	سرمد كوكب الجميل	المؤسسة المصرفية العربية: التحديات والخيارات في عصر العولمة
73.	أحمد سليم البرصان	عالم الجنوب: المفهوم وتحدياته
74.	محمد عبدالمعطي الجاويش	الرؤية الدولية لضبط انتشار أسلحة الدمار الشامل في الشرق الأوسط
75.	مازن خليل غرايبة	المجتمع المدني والتكامل: دراسة في التجربة العربية
76.	تركي راجي الحمود	التحديات التي تواجه المصارف الإسلامية في دولة قطر (دراسة ميدانية)
77.	أبوبكر سلطان أحمد	التحول إلى مجتمع معلوماتي: نظرة عامة
78.	سلمان قادم آدم فضل	حق تقرير المصير: طرح جديد لمبدأ قديم دراسة لحالات أريتريا - الصحراء الغربية - جنوب السودان
79.	ناظم عبدالواحد الجاسور	ألمانيا الموحدة في القرن الحادي والعشرين: صعود القمة والمحددات الإقليمية والدولية
80.	فيصل محمد خير الزراد	الرعاية الأسرية للمسنين في دولة الإمارات العربية المتحدة: دراسة نفسية اجتماعية ميدانية في إمارة أبوظبي
81.	جاسم يونس الحريري	دور القيادة الكاريزمية في صنع القرار الإسرائيلي: نموذج بن جوريون
82.	علي محمود الفكيكي	الجديد في علاقة الدولة بالصناعة في العالم العربي والتحديات المعاصرة

83.	عبدالمنعم السيد علي	العولمة من منظور اقتصادي وفرضية الاحتواء
84.	إبراهيم مصحب الدليمي	المخدرات والأمن القومي العربي (دراسة من منظار سوسيولوجي)
85.	سيار كوكب الجميل	المجال الحيوي للخليج العربي: دراسة جيواستراتيجية
86.	منار محمد الرشواني	سياسات التكيف الهيكلي والاستقرار السياسي في الأردن
87.	محمد علي داهش	اتجاهات العمل الوحدوي في المغرب العربي المعاصر
88.	محمد حسن محمد	الطاقة النووية وآفاقها السلمية في العالم العربي
89.	رضوان السيد	مسألة الحضارة والعلاقة بين الحضارات لدى المثقفين المسلمين في الأزمنة الحديثة
90.	هوشيار معروف	التنمية الصناعية في العالم العربي ومواجهة التحديات الدولية
91.	محمد الدعمي	الإسلام والعولمة: الاستجابة العربية - الإسلامية لمعطيات العولمة
92.	أحمد مصطفى جابر	اليهود الشرقيون في إسرائيل: جدل الضحية والجلاد
93.	هاني أحمد أبوقديس	استراتيجيات الإدارة المتكاملة للموارد المائية
94.	محمد هشام خواجكية وأحمد حسين الرفاعي	القطاع الخاص العربي في ظل العولمة وعمليات الاندماج: التحديات والفرص
95.	ثامر كامل محمد ونبيل محمد سليم	العلاقات التركية - الأمريكية والشرق الأوسط في عالم ما بعد الحرب الباردة
96.	مصطفى عبدالعزيز مرسي	الأهمية النسبية لخصوصية مجلس التعاون لدول الخليج العربية

97. علي مجيد الحمادي — الجهود الإنمائية العربية وبعض تحديات المستقبل
98. آرشاك بولاديان — مسألة أصل الأكراد في المصادر العربية
99. خليل إبراهيم الطيار — الصراع بين العلمانية والإسلام في تركيا
100. جهاد حرب عودة — المجلس التشريعي الفلسطيني للمرحلة الانتقالية: نحو تأسيس حياة برلمانية
101. محمد علي داهش ورواء زكي يونس — اتحاد المغرب العربي ومشكلة الأمن الغذائي: الواقع ومتطلبات المستقبل
102. عبدالله المجيدل — حقوق الطفل الاجتماعية والتربوية: دراسة ميدانية في سوريا
103. حسام الدين ربيع الإمام — البنك الدولي والأزمة المائية في الشرق الأوسط
104. شريف طلعت السعيد — مسار التجربة الحزبية في مصر (1974 – 1995)
105. علي عباس مراد — مشكلات الأمن القومي: نموذج تحليلي مقترح
106. عمار جفال — التنافس التركي – الإيراني في آسيا الوسطى والقوقاز
107. فتحي درويش عشيبة — الثقافة الإسلامية للطفل والعولمة
108. عدي قصيور — حماية حقوق المساهمين الأفراد في سوق أبوظبي للأوراق المالية
109. عمر أحمد علي — جدار الفصل في فلسطين: فكرته ومراحله – آثاره – وضعه القانوني
110. محمد خليل الموسى — التسويات السلمية المتعلقة بخلافة الدول وفقاً لأحكام القانون الدولي
111. محمد فايز فرحات — مجلس التعاون لدول الخليج العربية وعملية التكامل في منطقة المحيط الهندي: نحو سياسة خليجية جديدة

112. صفات أمين سلامة	أسلحة حروب المستقبل بين الخيال والواقع
113. وليد كاصد الزيدي	الفرانكفونية في المنطقة العربية: الواقع والآفاق المستقبلية
114. محمد عبدالباسط الشمنقي ومحمد حاجي	استشراف أولي لآثار تطبيق بروتوكول كيوتو بشأن تغير المناخ على تطور السوق العالمية للنفط
115. محمد المختار ولد السعد	عوائق الإبداع في الثقافة العربية بين الموروث الآسر وتحديات العولمة
116. ستار جبار علاي وخضر عباس عطوان	العراق: قراءة لوضع الدولة ولعلاقاتها المستقبلية
117. إبراهيم فريد عاكوم	إدارة الحكم والعولمة: وجهة نظر اقتصادية
118. نوزاد عبدالرحمن الهيتي	المساعدات الإنمائية المقدمة من دول مجلس التعاون لدول الخليج العربية: نظرة تحليلية
119. إبراهيم عبدالكريم	حزب كديما وحكومته الائتلافية: دراسة حالة في الخريطة السياسية الإسرائيلية وانعكاساتها
120. لقمان عمر النعيمي	تركيا والاتحاد الأوربي: دراسة لمسيرة الانضمام
121. محمد بن مبارك العريمي	الرؤية العُمانية للتعاون الخليجي
122. ماجد كيالي	مشروع الشرق الأوسط الكبير: دلالاته وإشكالاته
123. حسن الحاج علي أحمد	خصخصة الأمن: الدور المتنامي للشركات العسكرية والأمنية الخاصة
124. سعد غالب ياسين	نظم إدارة المعرفة ورأس المال الفكري العربي
125. عادل ماجد	مسؤولية الدول عن الإساءة للأديان والرموز الدينية
126. سهيلة عبد الأنيس محمد	العلاقات الإيرانية – الأوروبية: الأبعاد وملفات الخلاف

127.	ثامر كامل محمد	الأخلاقيات السياسية للنظام العالمي الجديد ومعضلة النظام العربي
128.	فاطمة حافظ	تمكين المرأة الخليجية: جدل الداخل والخارج
129.	مصطفى علوي سيف	استراتيجية حلف شمال الأطلسي تجاه منطقة الخليج العربي
130.	محمد بوبوش	قضية الصحراء ومفهوم الحكم الذاتي: وجهة نظر مغربية
131.	راشد بشير إبراهيم	التحقيق الجنائي في جرائم تقنية المعلومات: دراسة تطبيقية على إمارة أبوظبي

قواعد النشر

أولاً: القواعد العامة

1. تقبل البحوث ذات الصلة بالدراسات الاستراتيجية، وباللغة العربية فحسب.
2. يشترط ألا يكون البحث قد سبق نشره، أو قدم للنشر في جهات أخرى.
3. يراعى في البحث اعتماد الأصول العلمية والمنهجية المتعارف عليها في كتابة البحوث الأكاديمية.
4. يتعين ألا يزيد عدد صفحات البحث على 40 صفحة مطبوعة (A4)، بما في ذلك الهوامش، والمراجع، والملاحق.
5. يقدم البحث مطبوعاً في نسخة واحدة، بعد مراجعته من الأخطاء الطباعية.
6. يرفق الباحث بياناً موجزاً بسيرته العلمية، وعنوانه بالتفصيل، ورقم الهاتف والفاكس (إن وجد).
7. على الباحث أن يقدم موافقة الجهة التي قدمت له دعماً مالياً، أو مساعدة علمية (إن وجدت).
8. تكتب الهوامش بأرقام متسلسلة، وتوضع في نهاية البحث مع قائمة المراجع.
9. تطبع الجداول والرسوم البيانية على صفحات مستقلة، مع تحديد مصادرها، ويشار إلى مواقعها في متن البحث.
10. تقوم هيئة التحرير بالمراجعة اللغوية، وتعديل المصطلحات بالشكل الذي لا يخل بمحتوى البحث أو مضمونه.
11. يراعى عند كتابة الهوامش ما يلي:
الكتب: المؤلف، عنوان الكتاب (مكان النشر: دار النشر، سنة النشر)، الصفحة.
الدوريات: المؤلف، «عنوان البحث»، اسم الدورية، العدد (مكان النشر: تاريخ النشر)، الصفحة.

ثانياً: إجراءات النشر

1. ترسل البحوث والدراسات باسم رئيس تحرير «دراسات استراتيجية».
2. يتم إخطار الباحث بما يفيد تسلم بحثه خلال شهر من تاريخ التسلم.
3. يرسل البحث إلى ثلاثة محكّمين من ذوي الاختصاص في مجال البحث بعد إجازته من هيئة التحرير، على أن يتم التحكيم في مدة لا تتجاوز أربعة أسابيع من تاريخ إرسال البحث للتحكيم.
4. يخطر الباحث بقرار صلاحية البحث للنشر من عدمها خلال ثمانية أسابيع على الأكثر من تاريخ تسلم البحث.
5. في حالة ورود ملاحظات من المحكمين ترسل الملاحظات إلى الباحث لإجراء التعديلات اللازمة، على أن تعاد خلال مدة أقصاها شهر.
6. تصبح البحوث والدراسات المنشورة ملكاً لمركز الإمارات للدراسات والبحوث الاستراتيجية، ولا يحق للباحث إعادة نشرها في مكان آخر دون الحصول على موافقة كتابية من المركز.
7. إن أي ملاحظات ترد حول الدراسة بحدوث ممارسات مخالفة للأعراف الأكاديمية يكشفها المحكمون سوف تكون سبباً لرفض الدراسة فوراً، ويحتفظ مركز الإمارات للدراسات والبحوث الاستراتيجية بحقه في رفض أي عمل آخر يقدمه الباحث المعني لاحقاً.

قسيمة اشتراك في سلسلة

«دراسات استراتيجية»

الاســـم : ....

المؤسسة : ....

العنوان : ....

ص. ب : .... المدينــة: ....

الرمز البريدي: ....

الــدولـة : ....

هــاتـف : .... فــاكـس: ....

البريد الإلكتروني: ....

بدء الاشتراك: (من العدد: .... إلى العدد: ....)

رسوم الاشتراك*

للأفراد:	220 درهماً	60 دولاراً أمريكياً
للمؤسسات:	440 درهماً	120 دولاراً أمريكياً

- ❑ للاشتراك من داخل الدولة يقبل الدفع النقدي، والشيكات، والحوالات النقدية.
- ❑ للاشتراك من خارج الدولة تقبل فقط الحوالات المصرفية، مع تحمل المشترك تكاليف التحويل.
- ❑ في حالة الحوالة المصرفية، يرجى تحويل قيمة الاشتراك إلى حساب مركز الإمارات للدراسات والبحوث الاستراتيجية رقم 1950050565 ـ بنك أبوظبي الوطني ـ فرع الخالدية، ص. ب: 46175 أبـوظبي ـ دولـة الإمارات العربية المتحدة.
- ❑ يمكن الاشتراك عبر موقعنا على الإنترنت (www.ecssr.ae) باستعمال بطاقتي الائتمان Visa و Master Card.

لمزيد من المعلومات حول آلية الاشتراك يرجى الاتصال:

قسم التوزيع والمعارض

ص.ب: 4567 أبوظبي ـ دولة الإمارات العربية المتحدة

هاتف: 4044445 (9712) فاكس: 4044443 (9712)

البريد الإلكتروني: books@ecssr.ae

الموقع على الإنترنت: http://www.ecssr.ae

* تشمل رسوم الاشتراك الرسوم البريدية، وتغطي تكلفة اثني عشر عدداً من تاريخ بدء الاشتراك.

ISSN 1682-1203





مركز الإمارات للدراسات والبحوث الاستراتيجية

ص.ب. 4567 - أبوظبي - إ.ع.م. - هاتف: 4044541 -2- 971- فاكس: 4044542 -2- 971- E-mail: pubdis@ecssr.ae